

This page is not part of
the document!

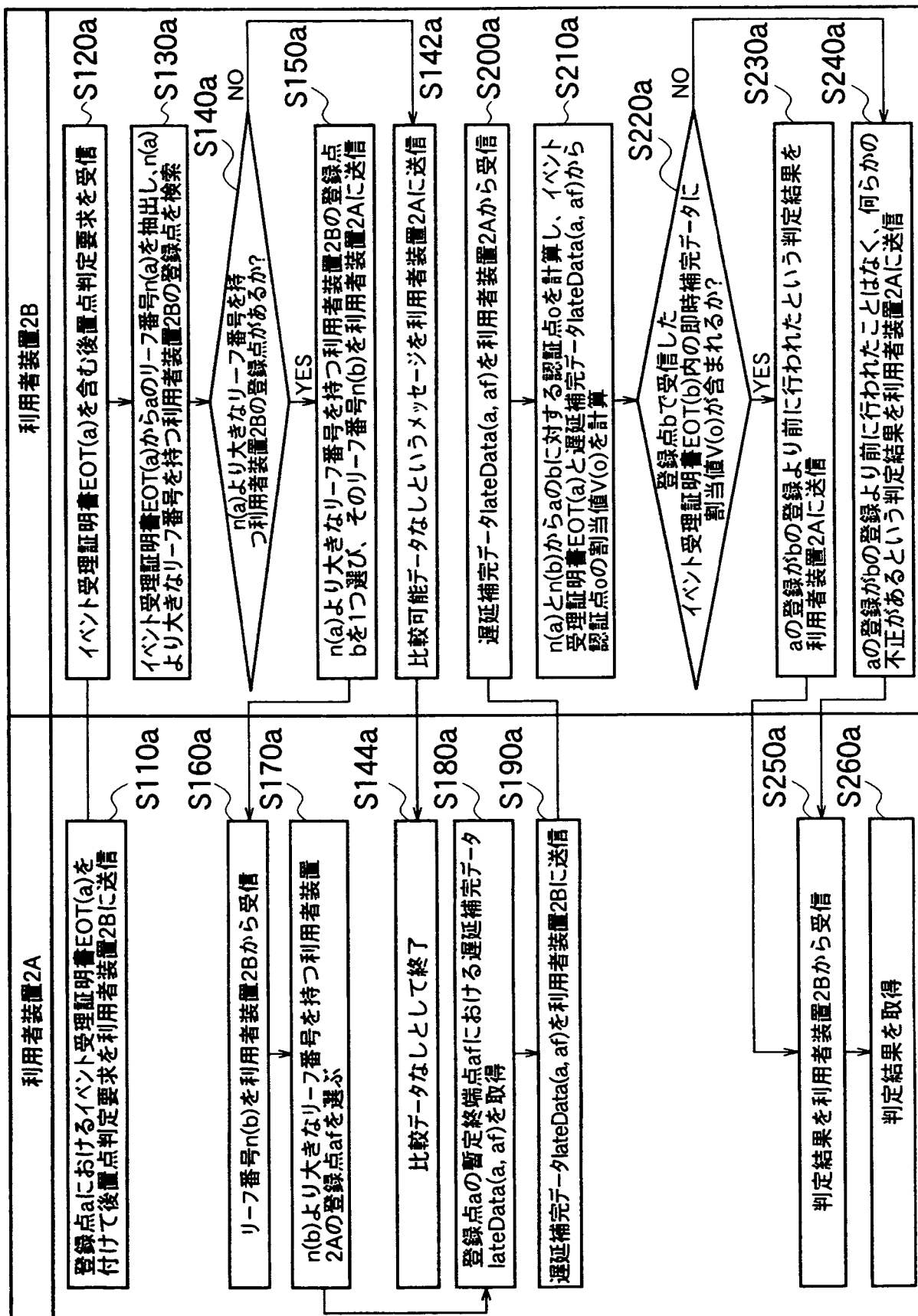
JP2005015085 / 2006-019143

3/3

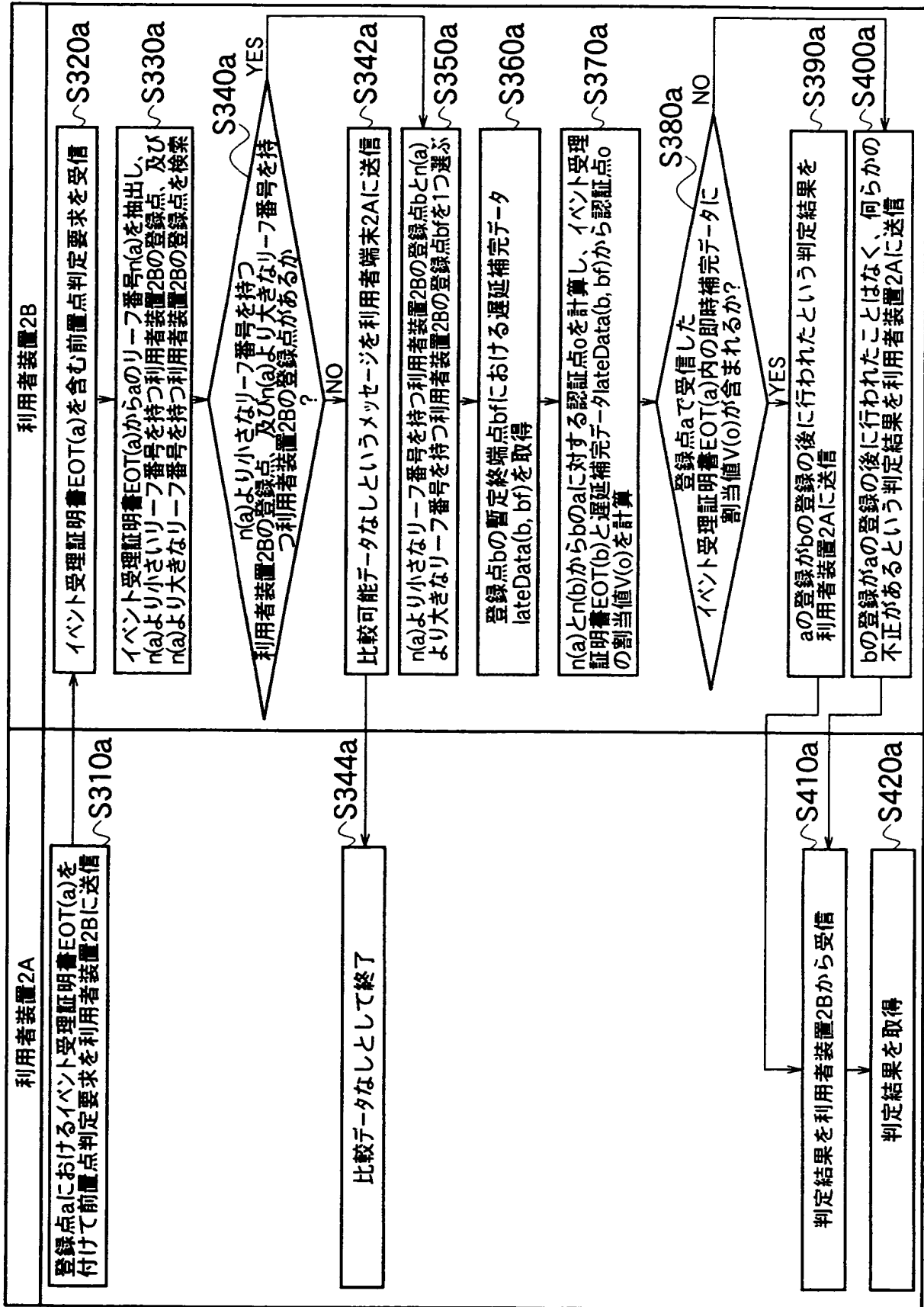
Date: Feb 23, 2006

Recipient: IB

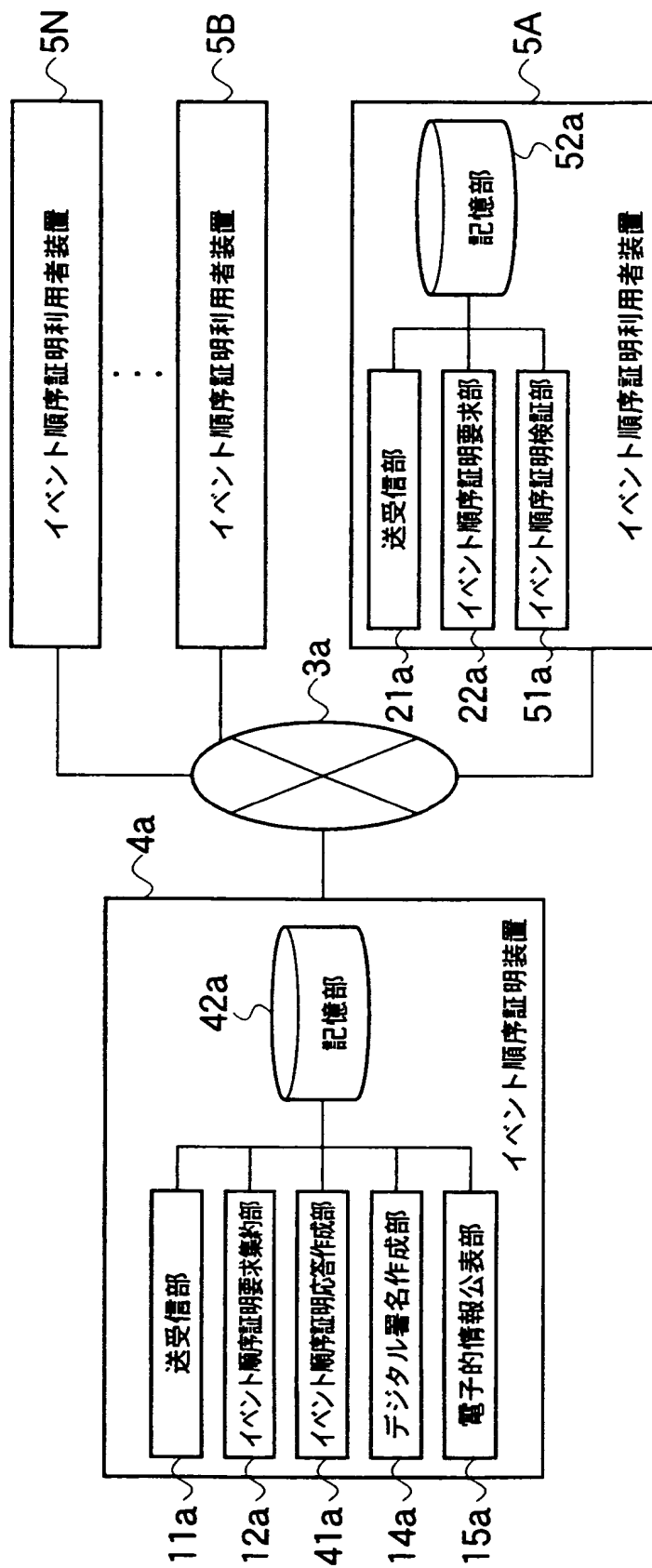
[図40]



[図41]



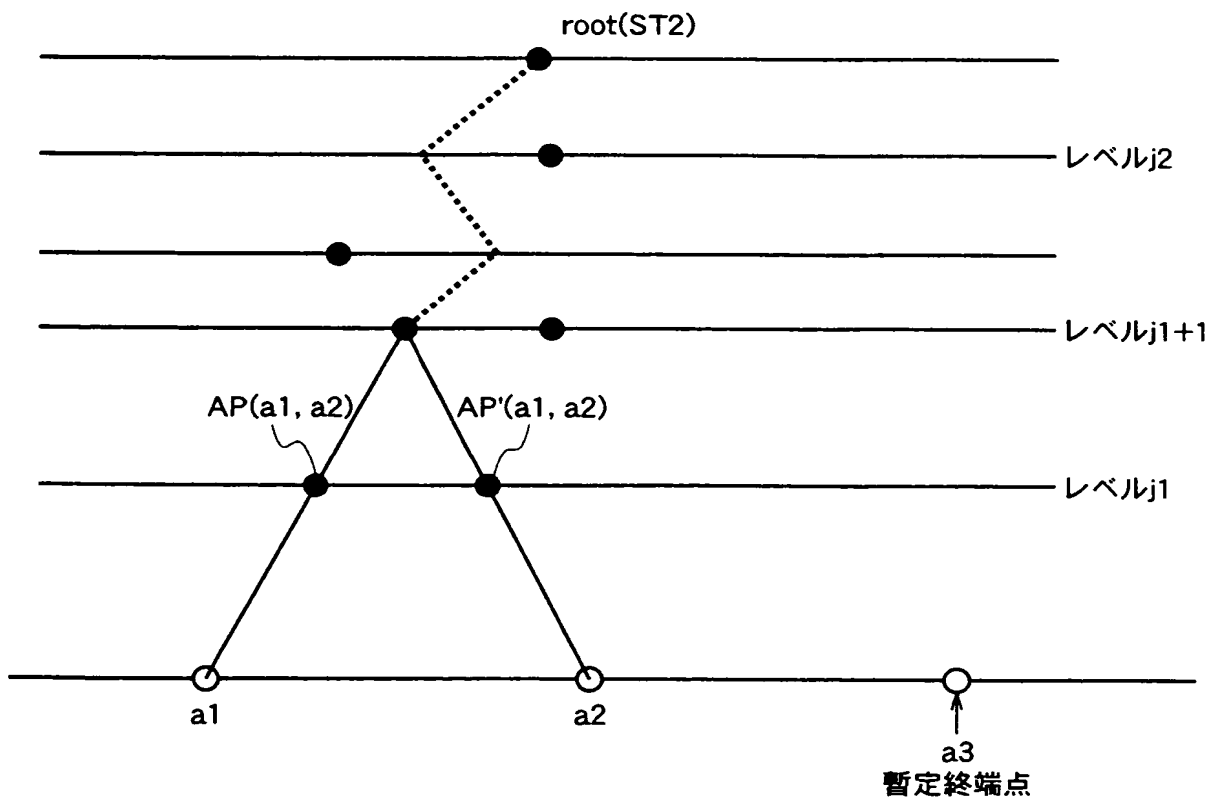
[図42]



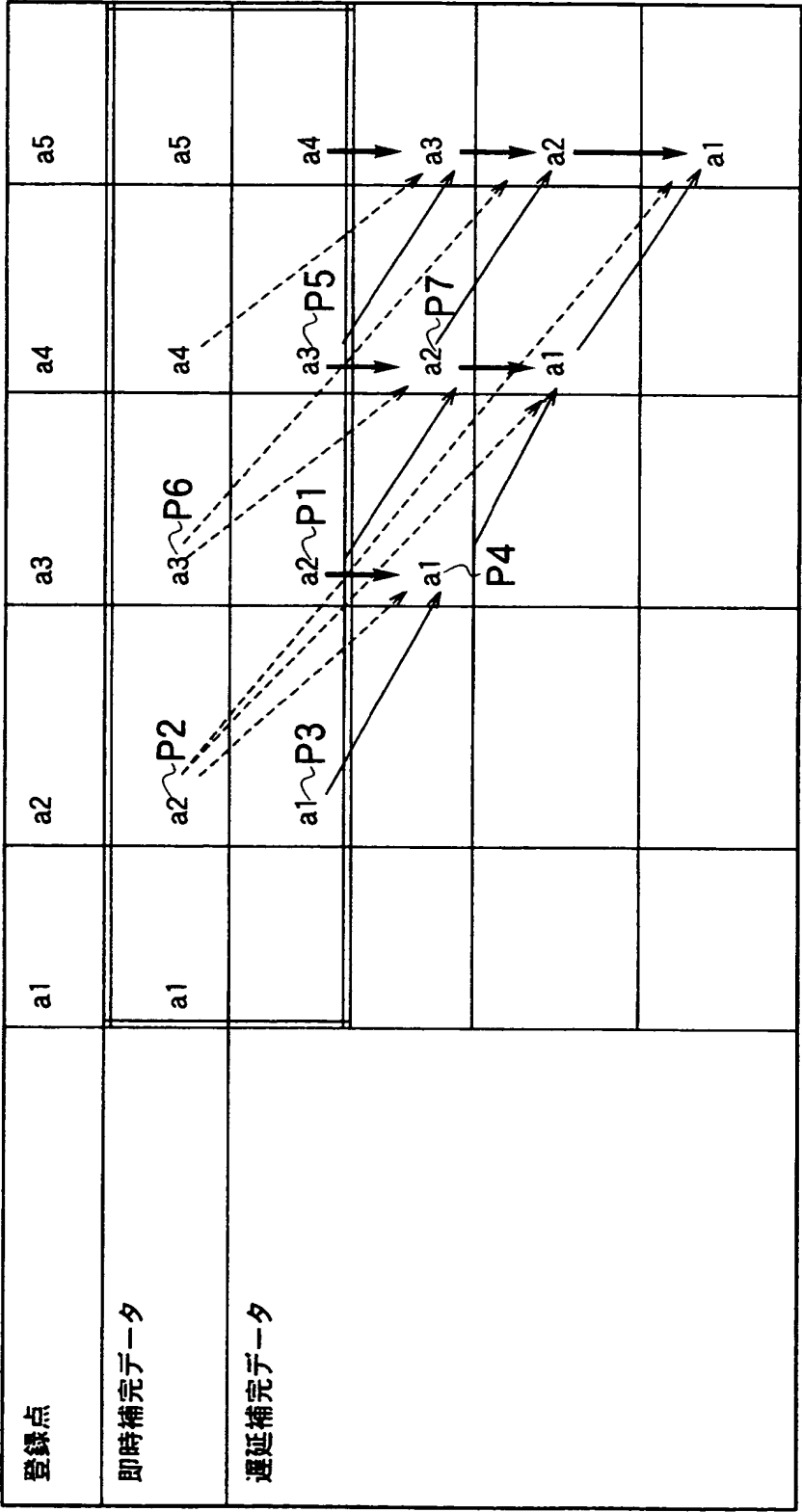
[図43]

項目	記号	必須	イベント順序受理証明書 EOC(y)
元デジタルデータ	y	○	
順次割当データ	z	○	
順次集約木識別番号	n	○	
順次集約木リーフ番号	i	○	
登録点の即時補完データ(位置情報、割当値)	SK	○	
直前登録点の遅延補完データ(位置情報、割当値)	TK2	○	

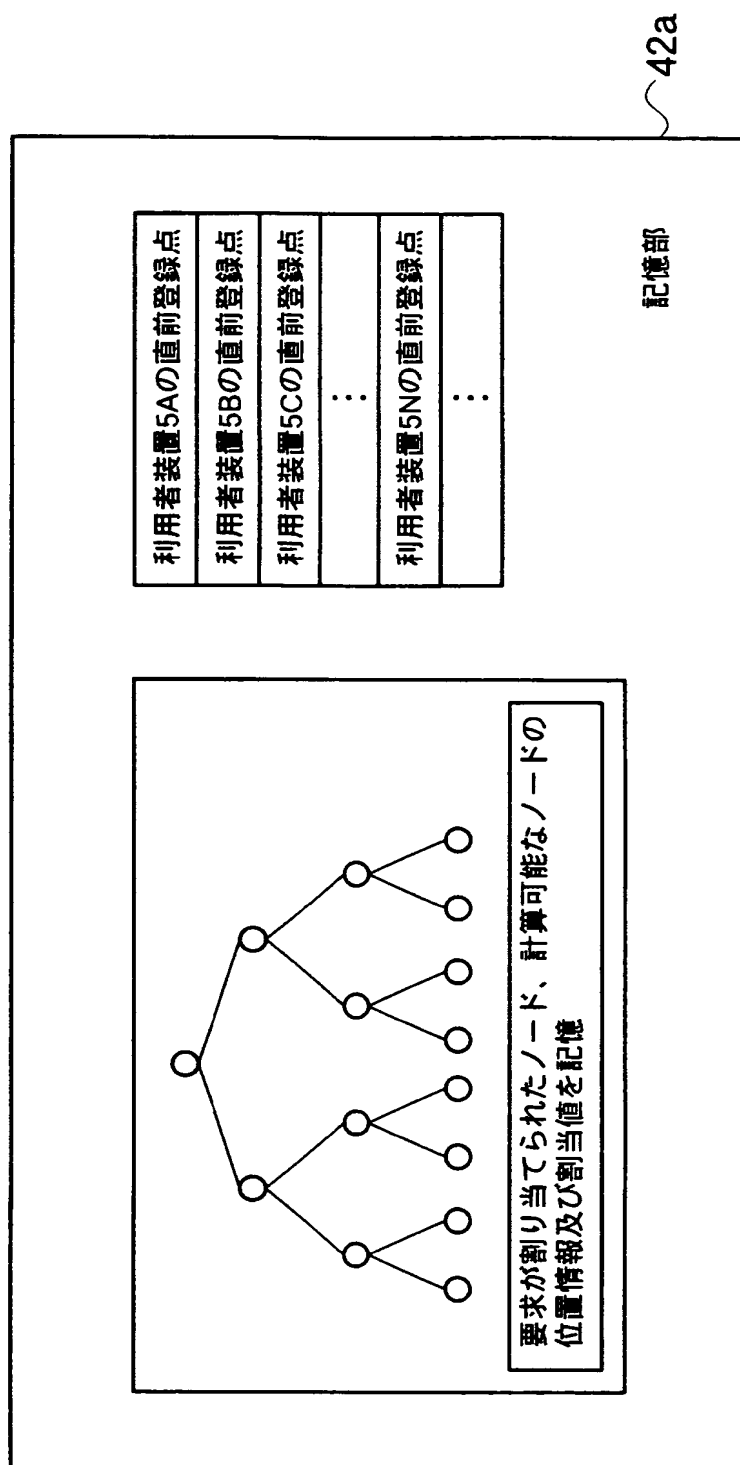
[図44]



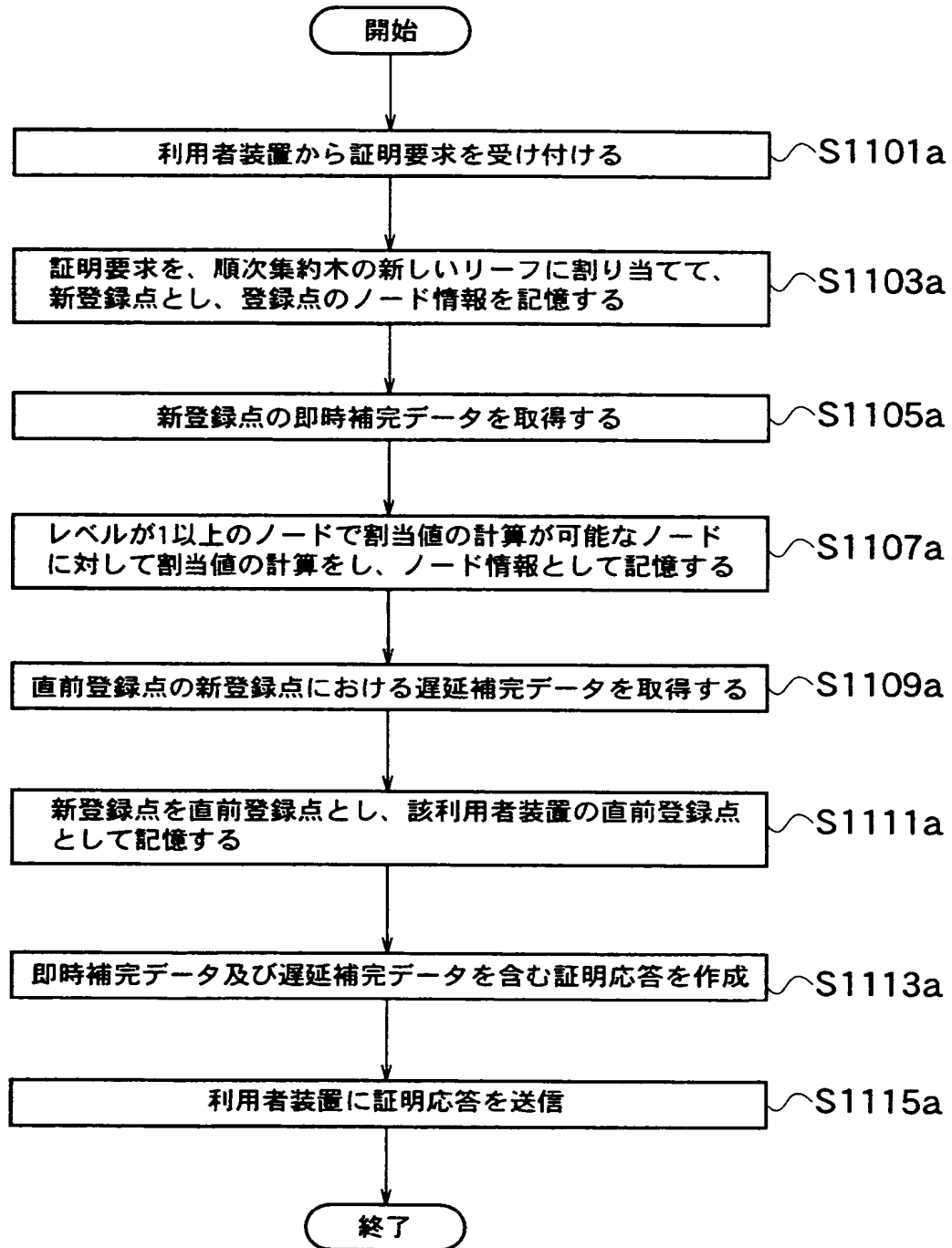
[図45]



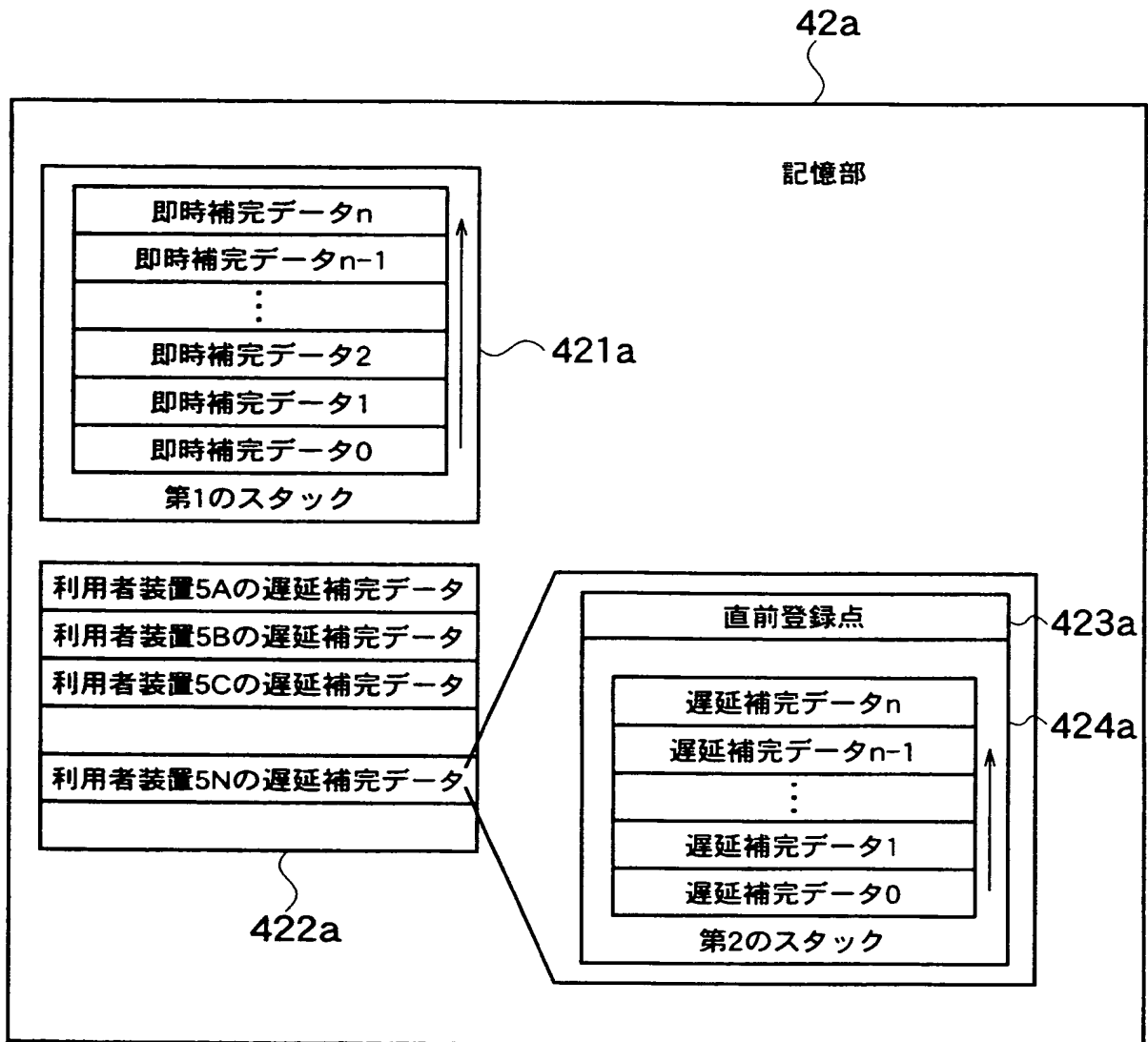
[図46]



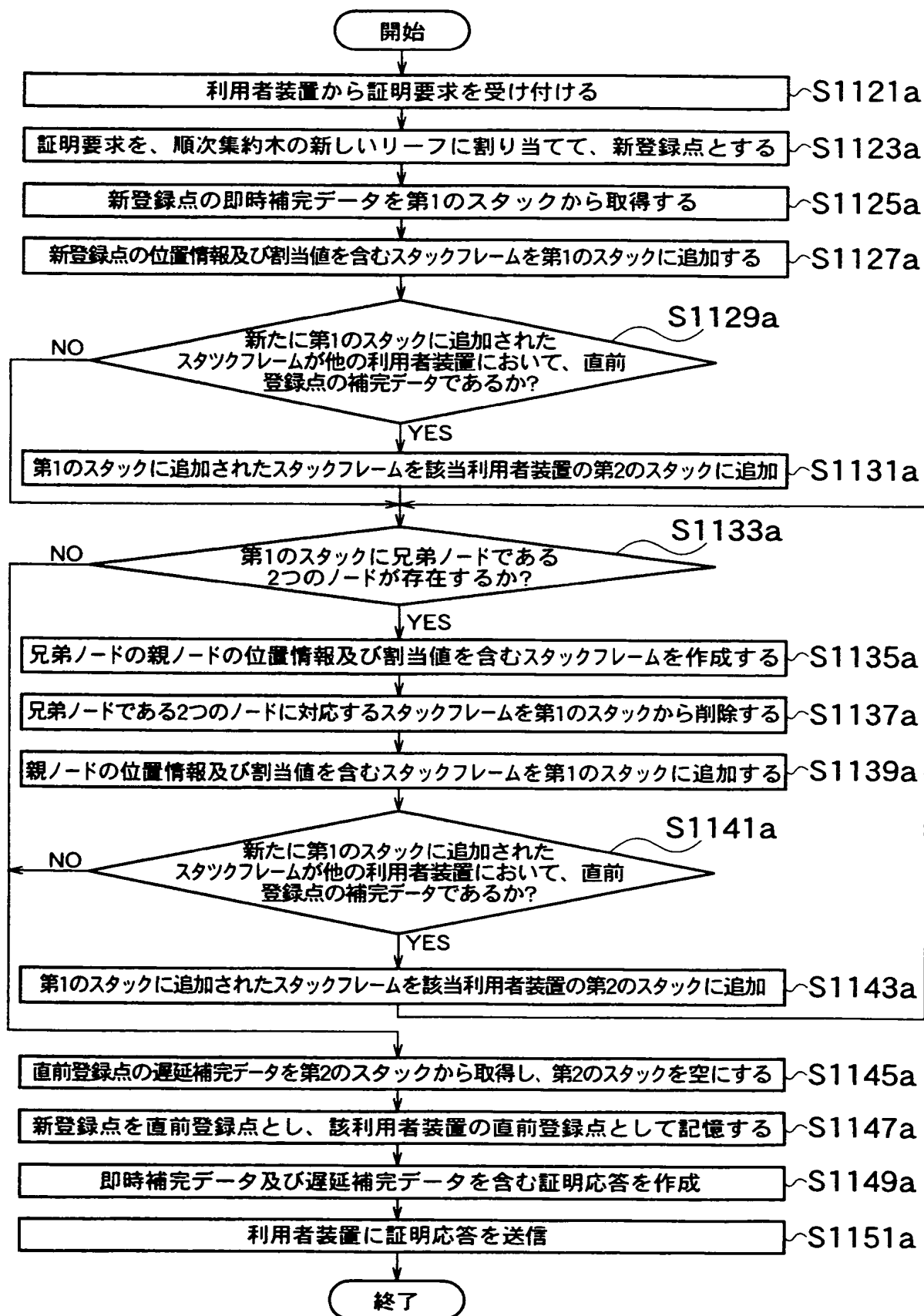
[図47]



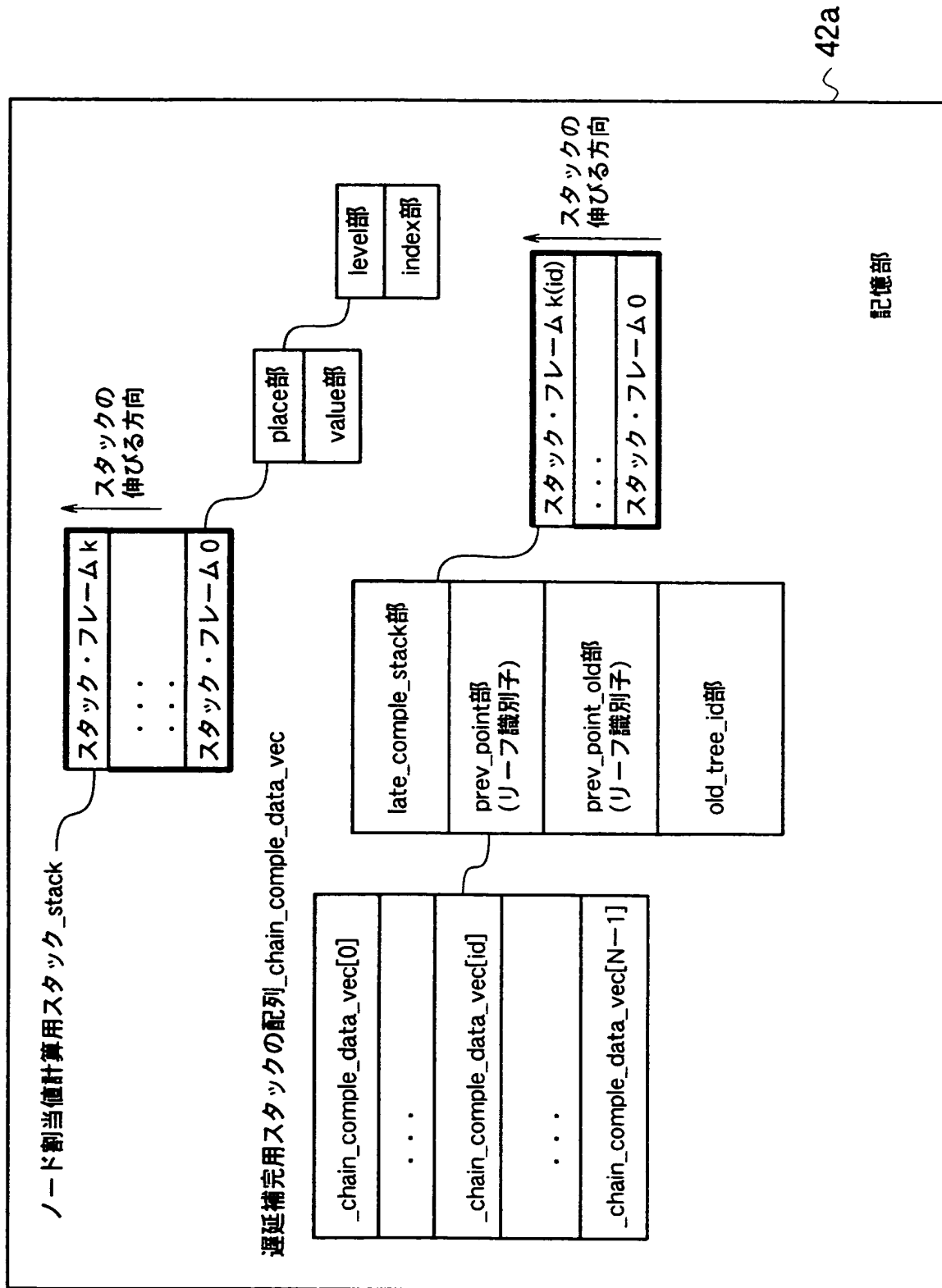
[図48]



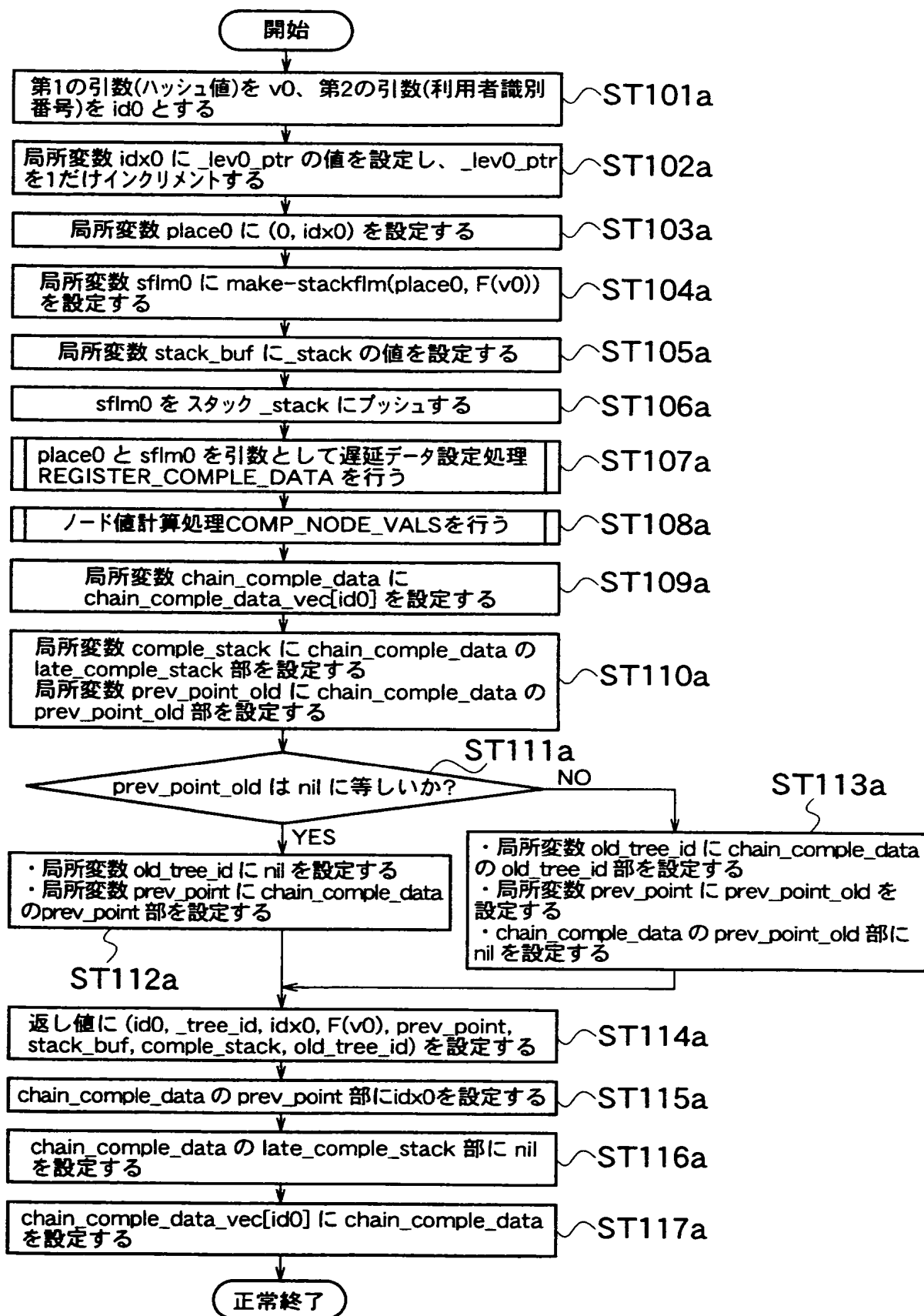
[図49]



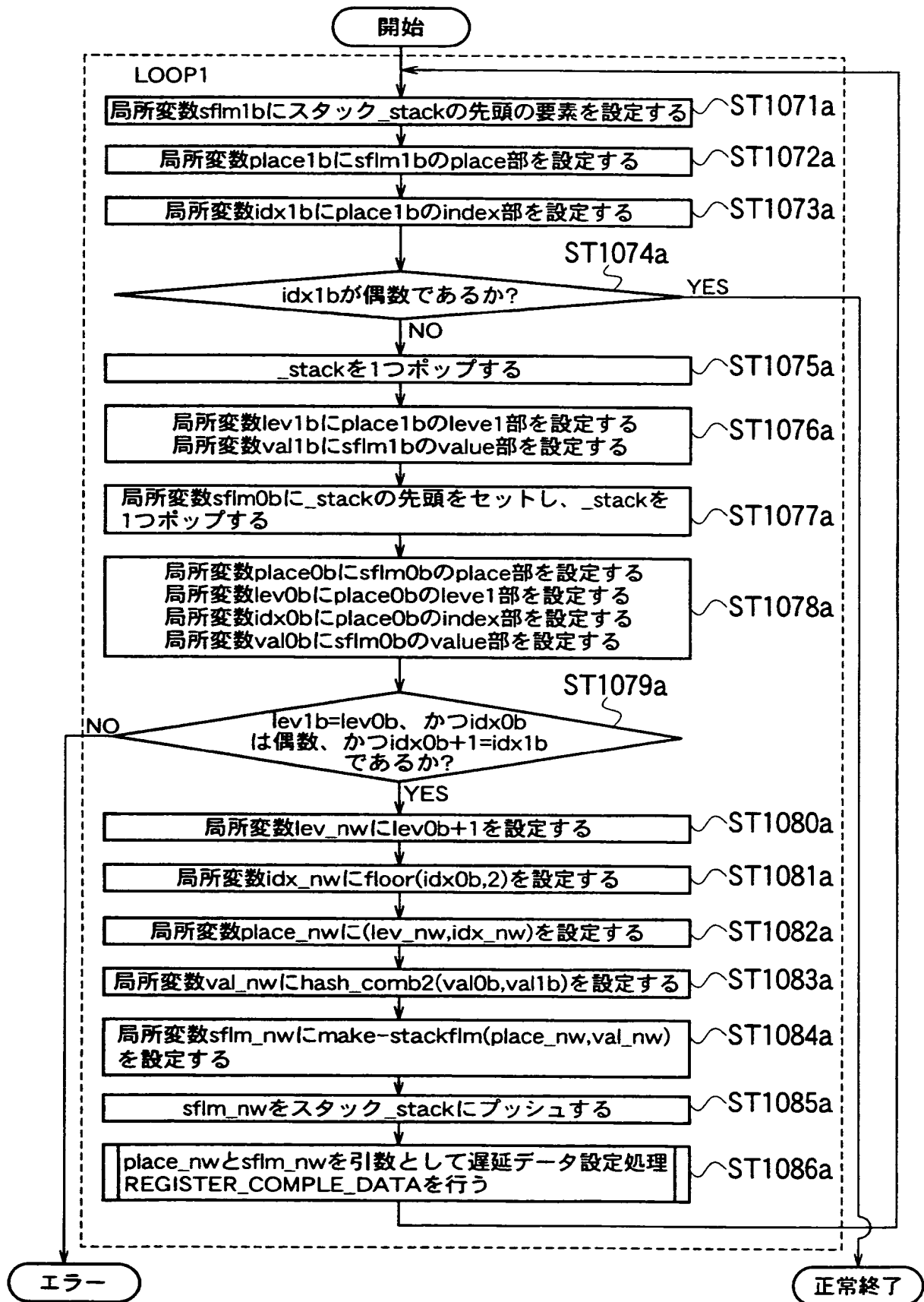
[[図50]



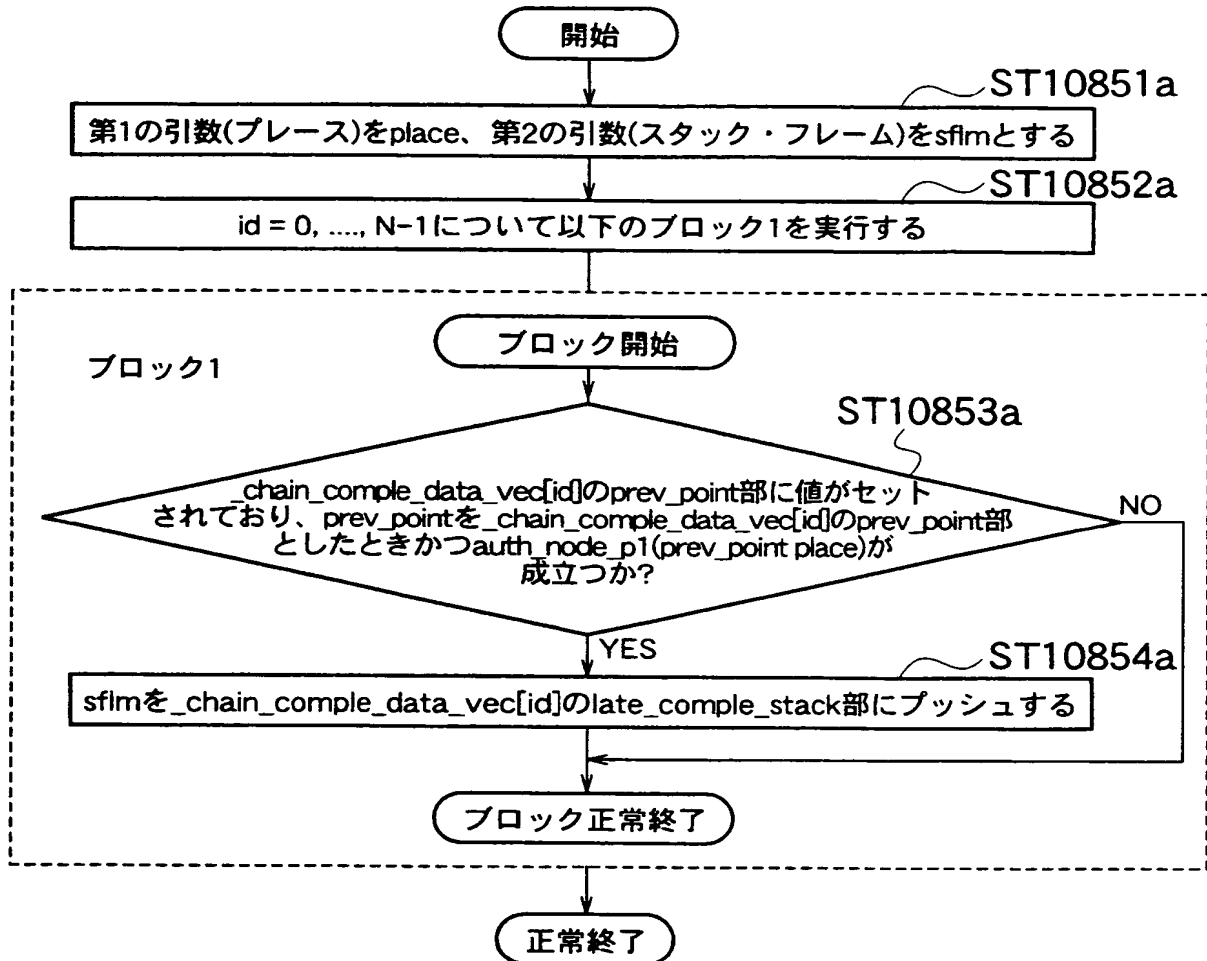
[図51]



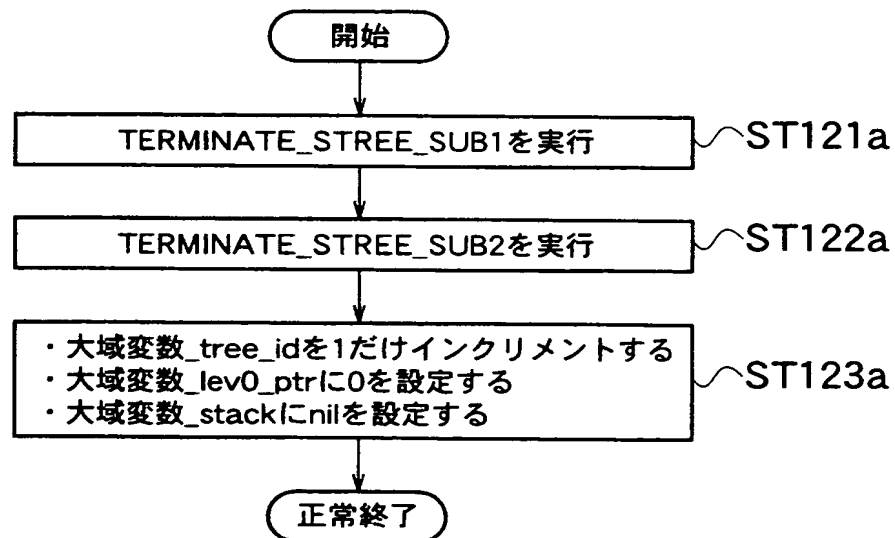
[図52]



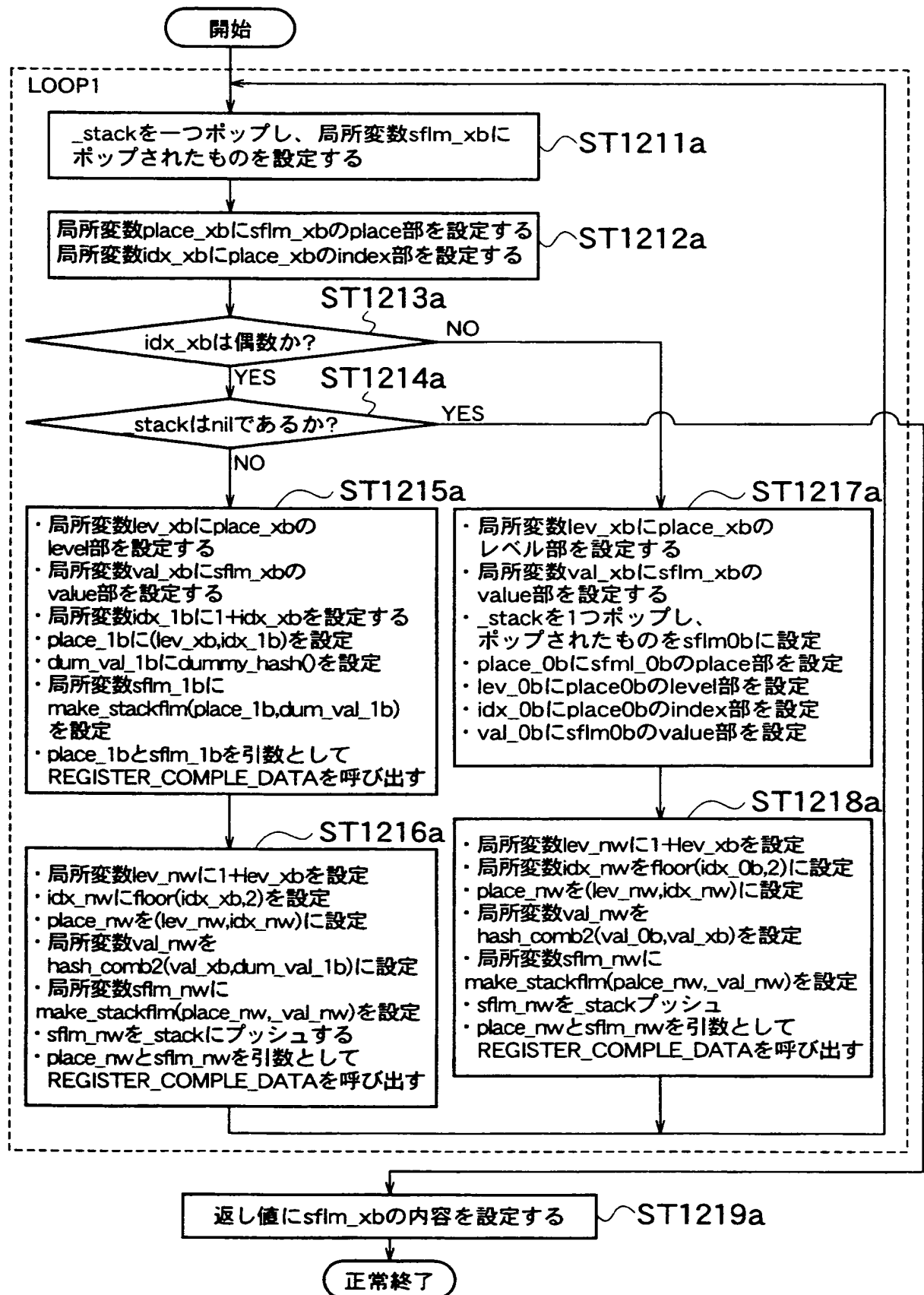
[図53]



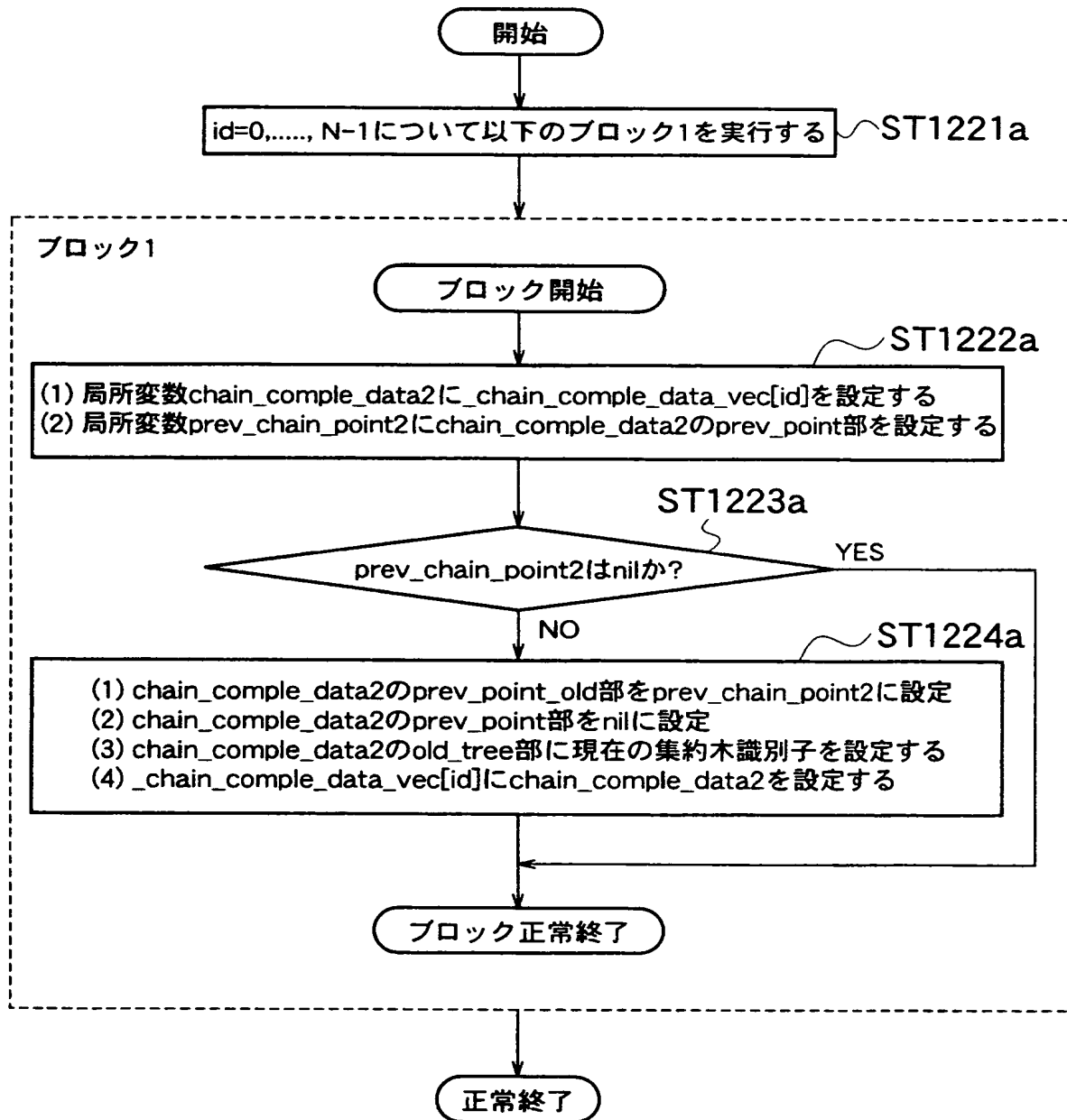
[図54]



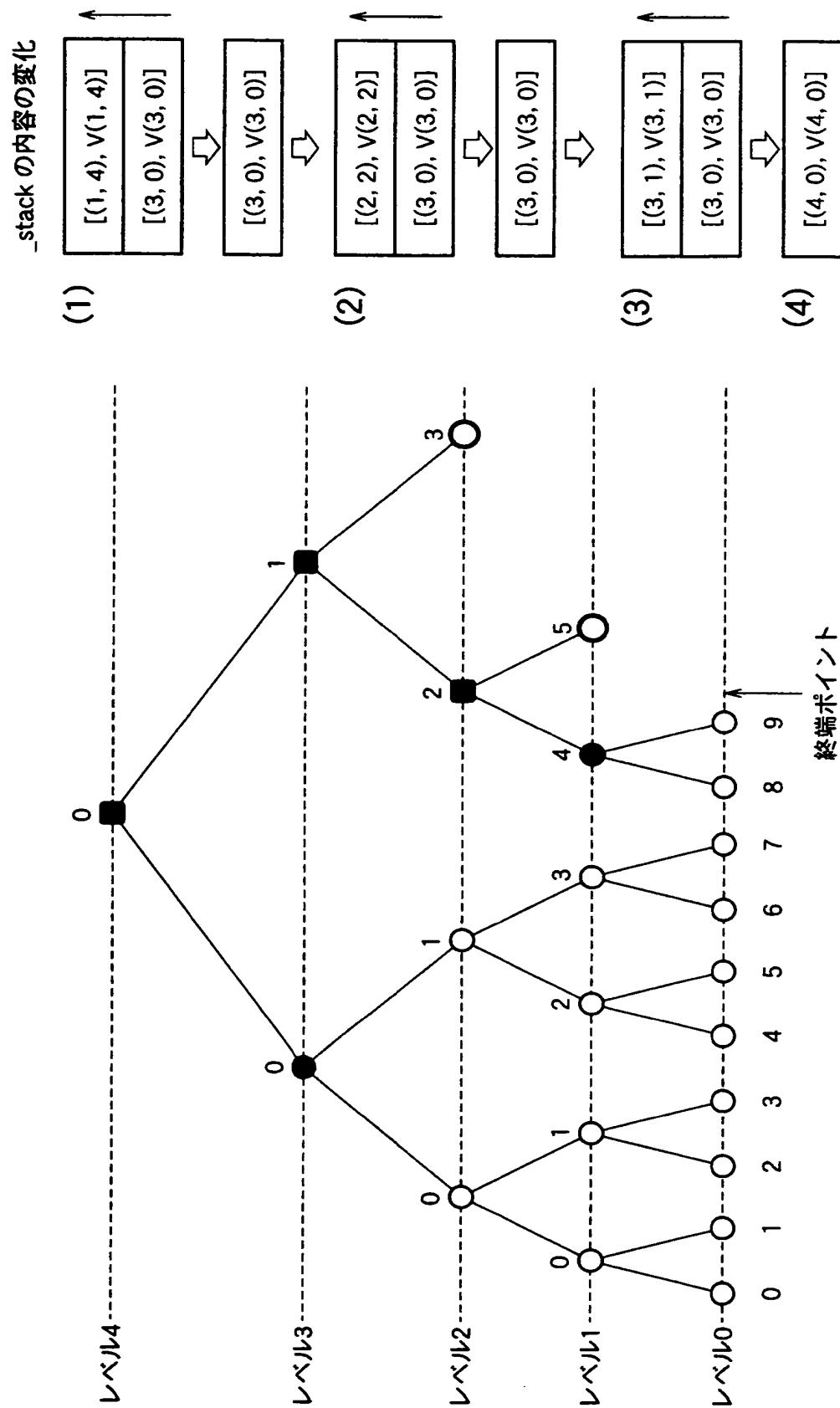
[図55]



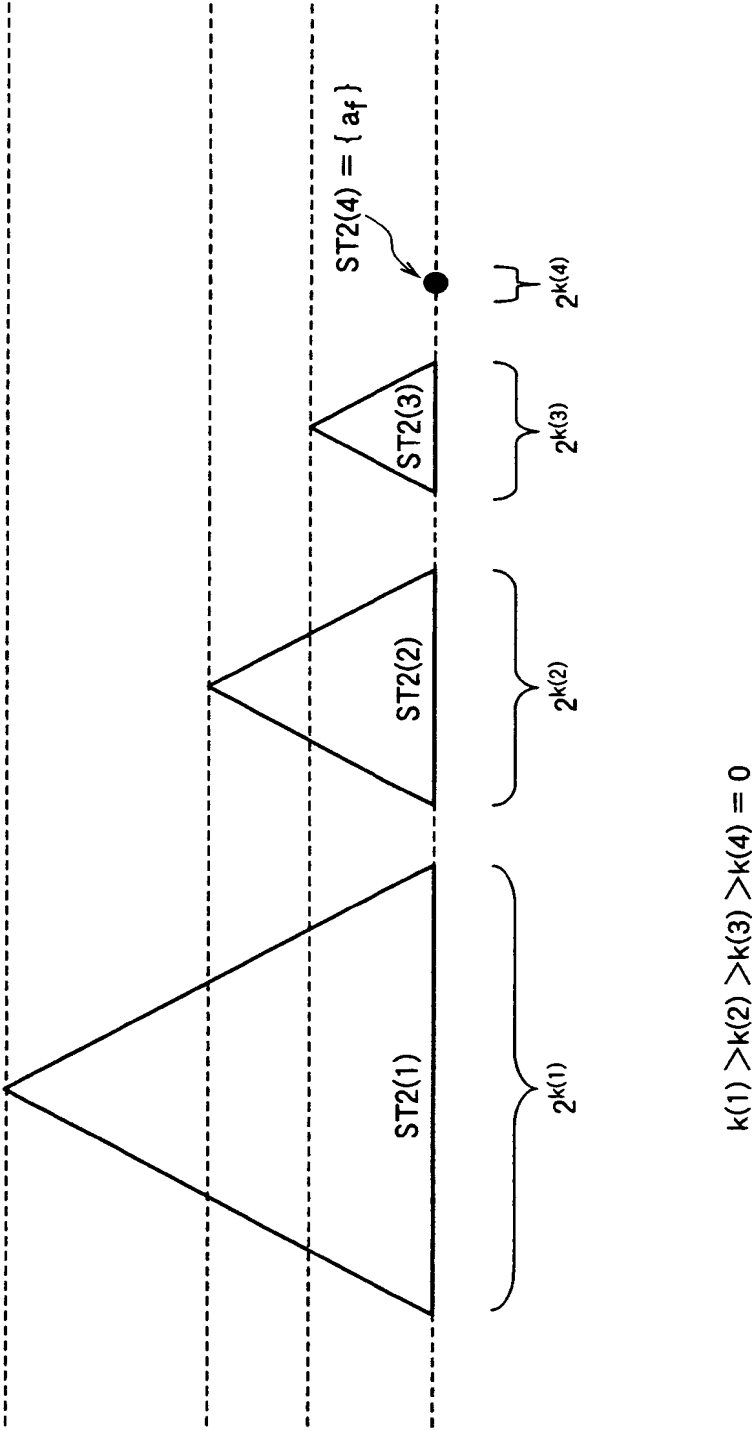
[図56]



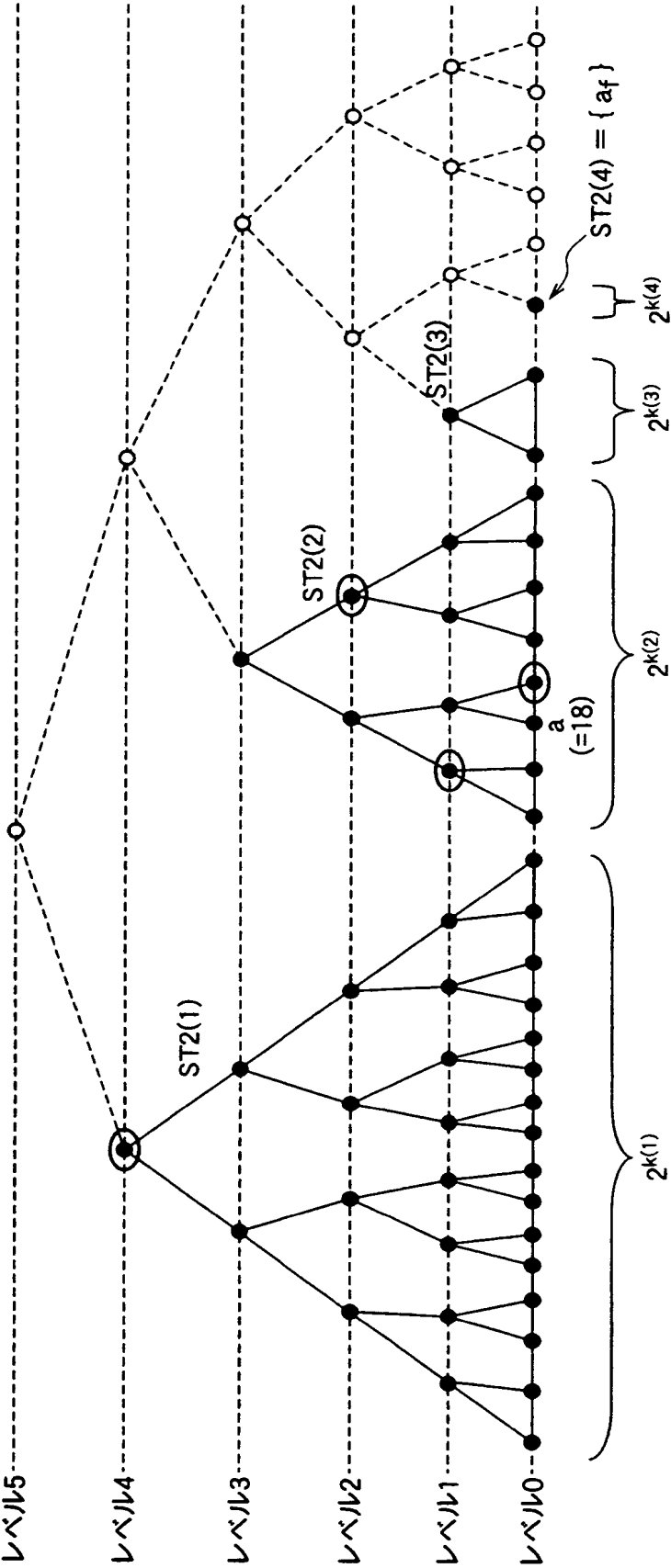
[図57]



[図58]

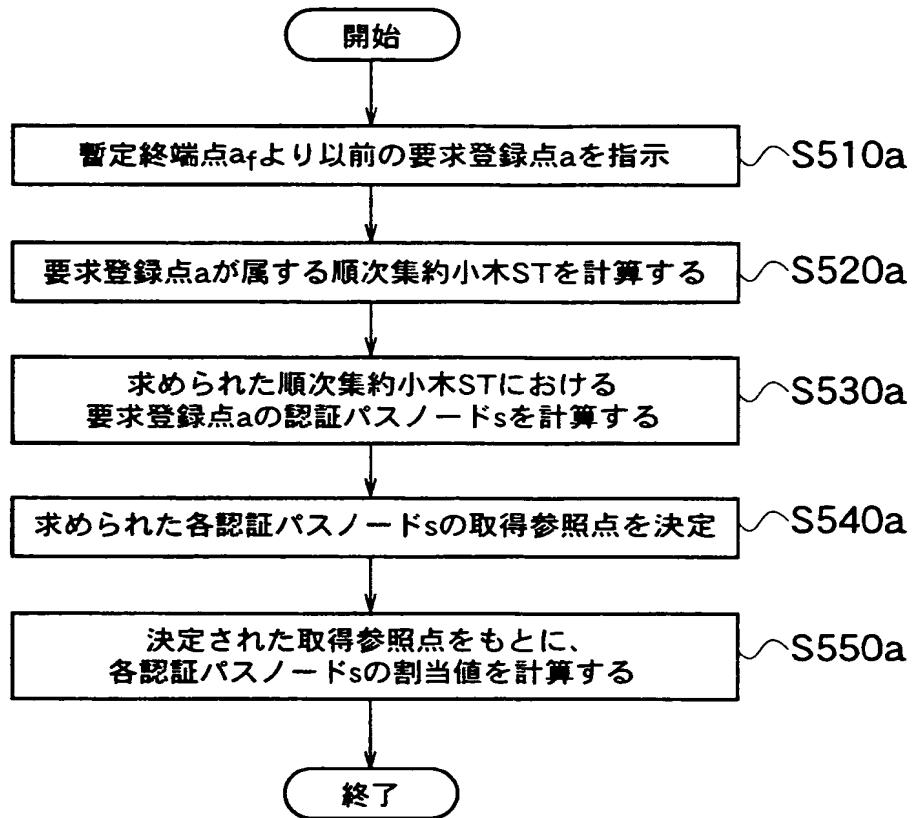


[図59]

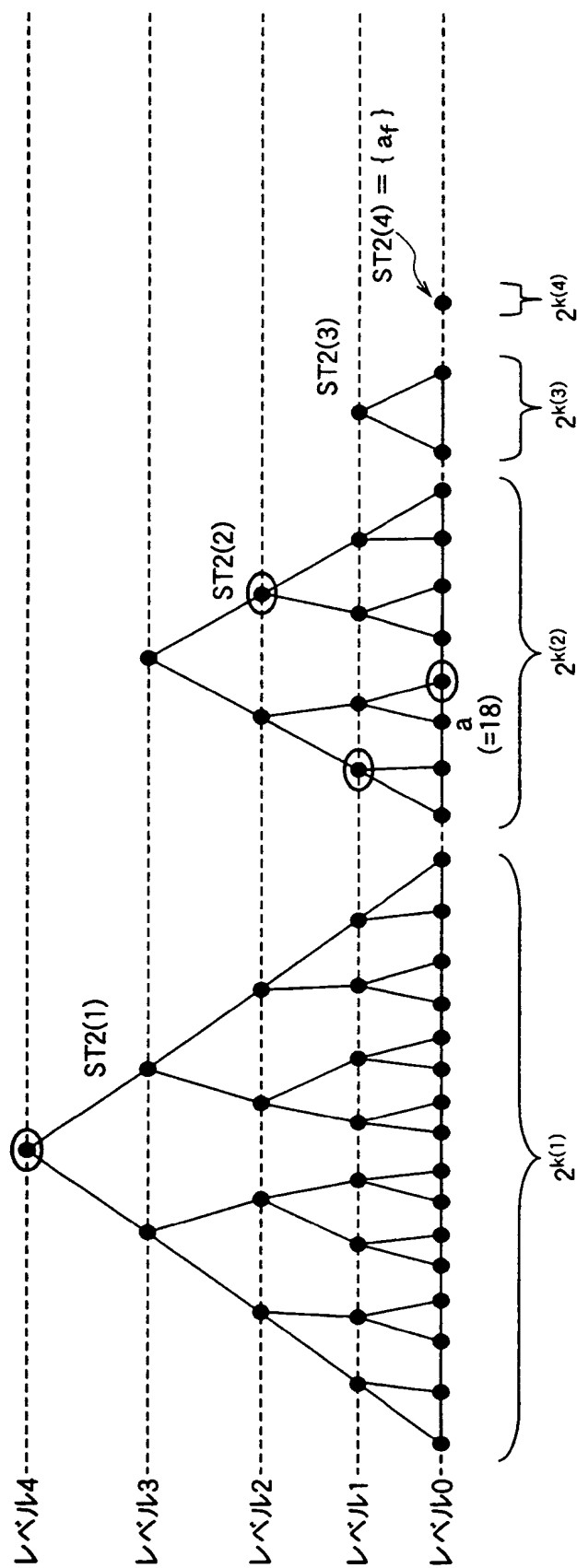


$$k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0$$

[図60]

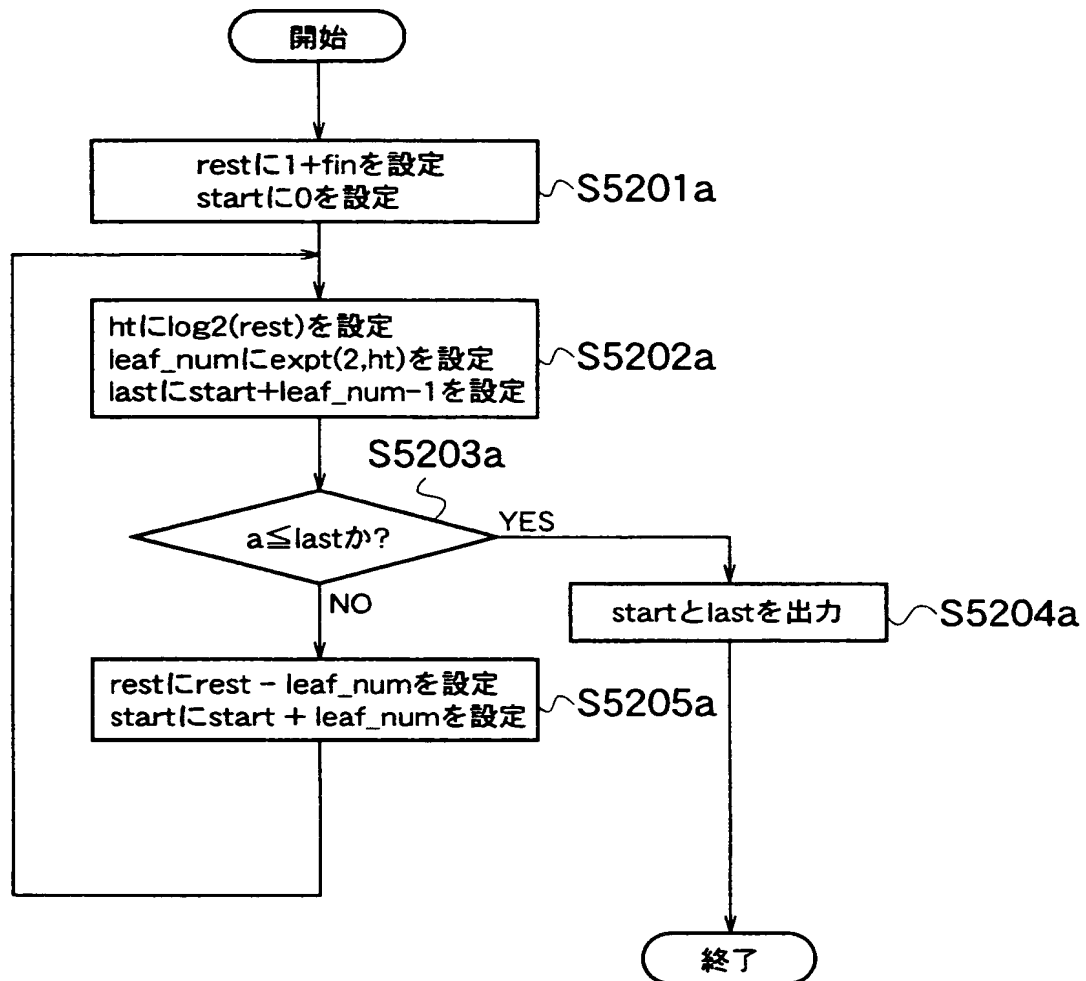


[図61]

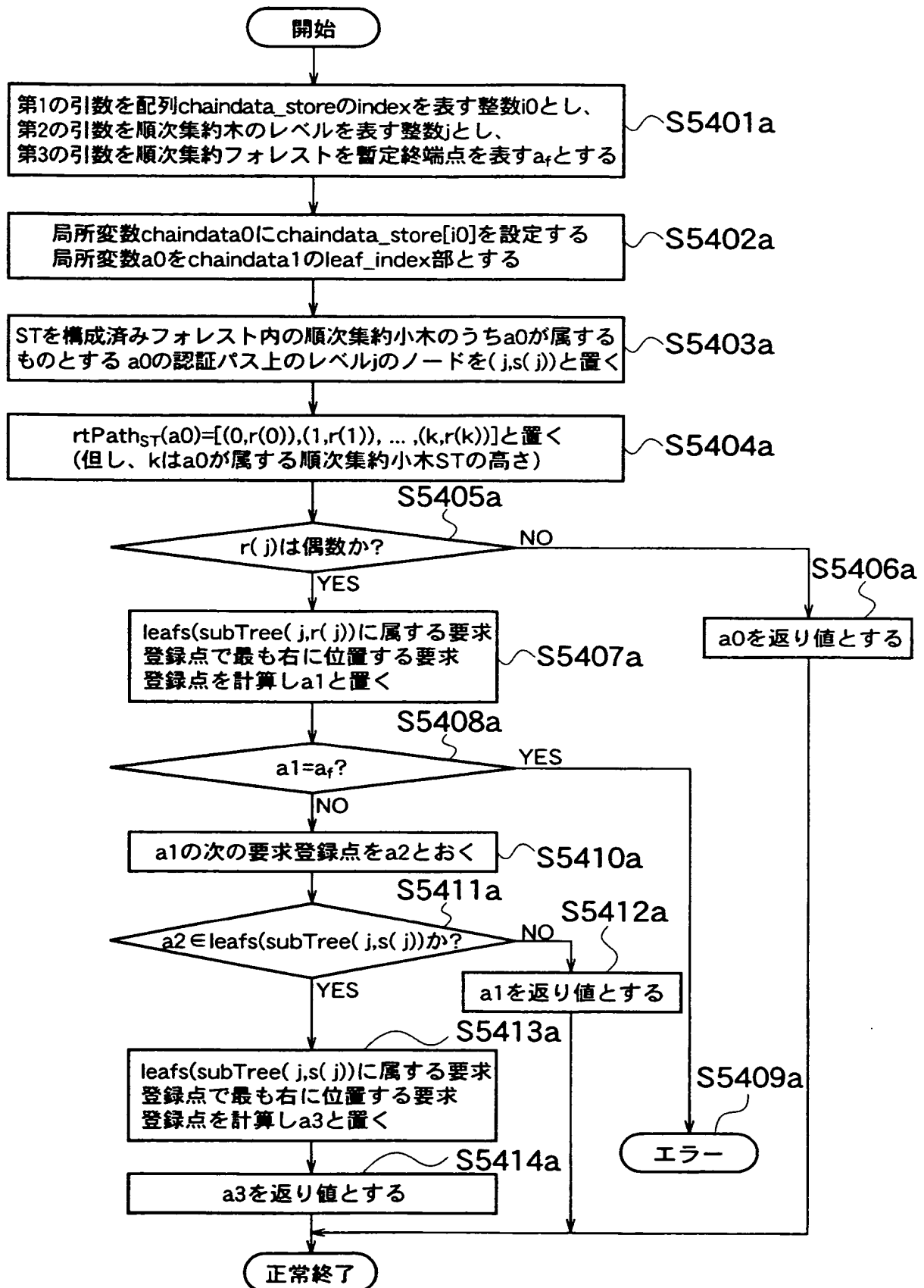


$$k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0$$

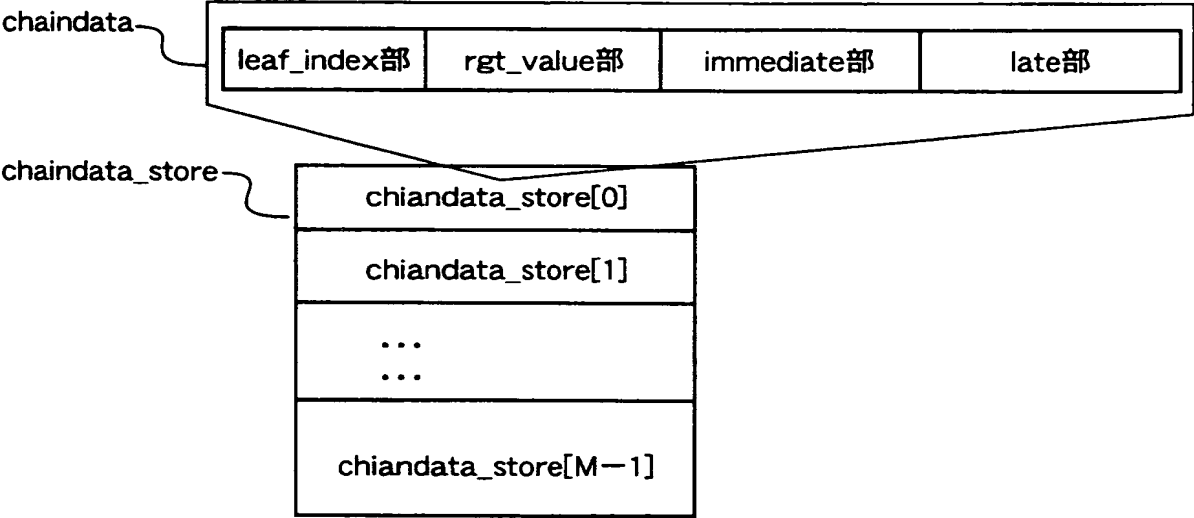
[図62]



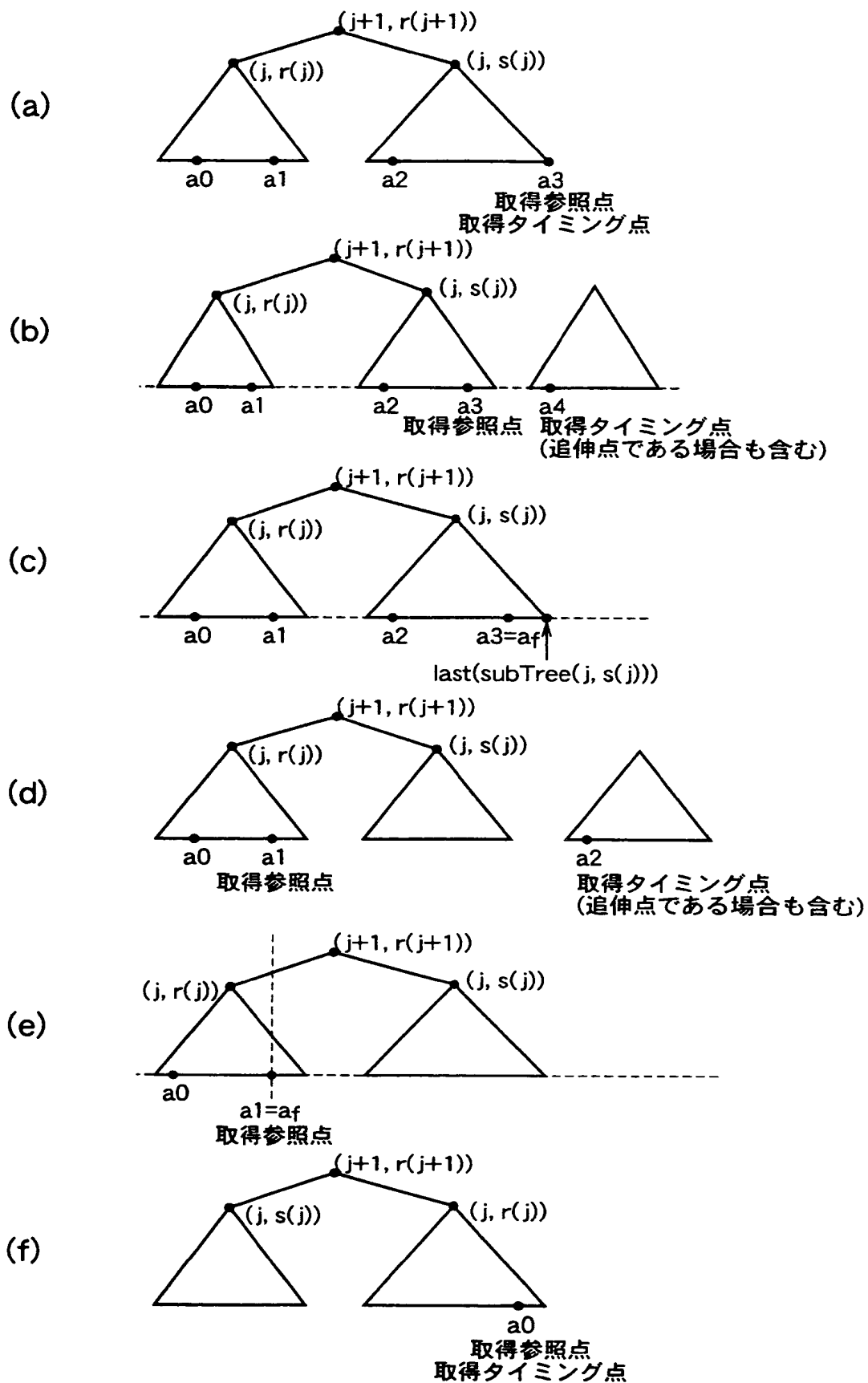
[図63]



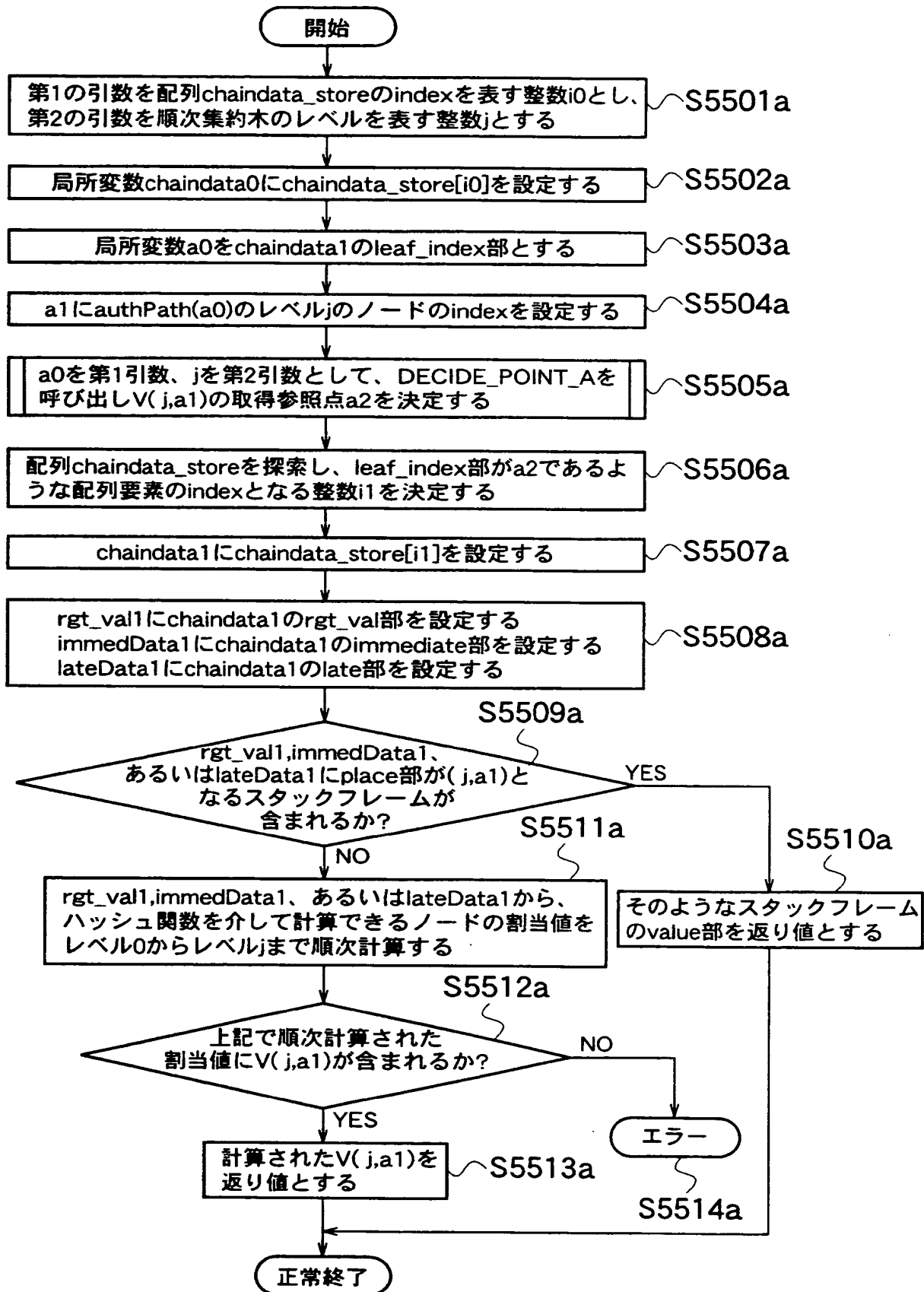
[図64]



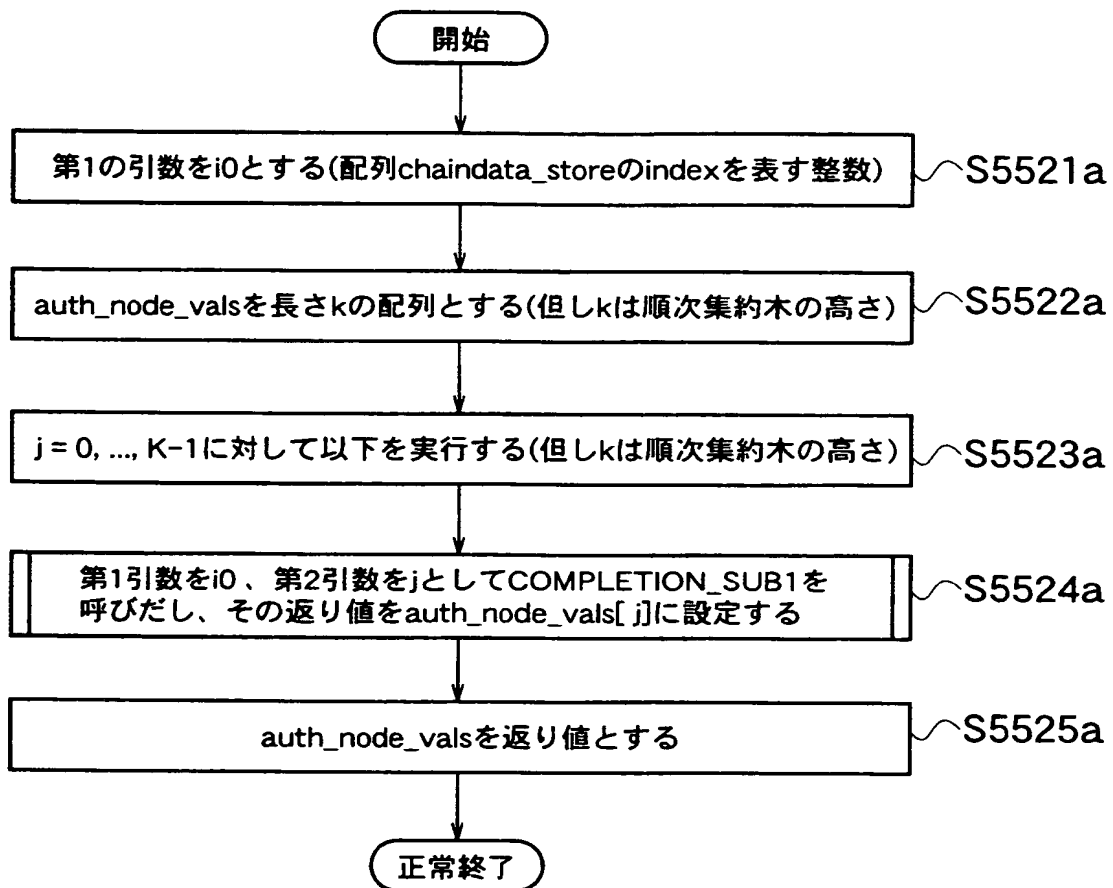
[図65]



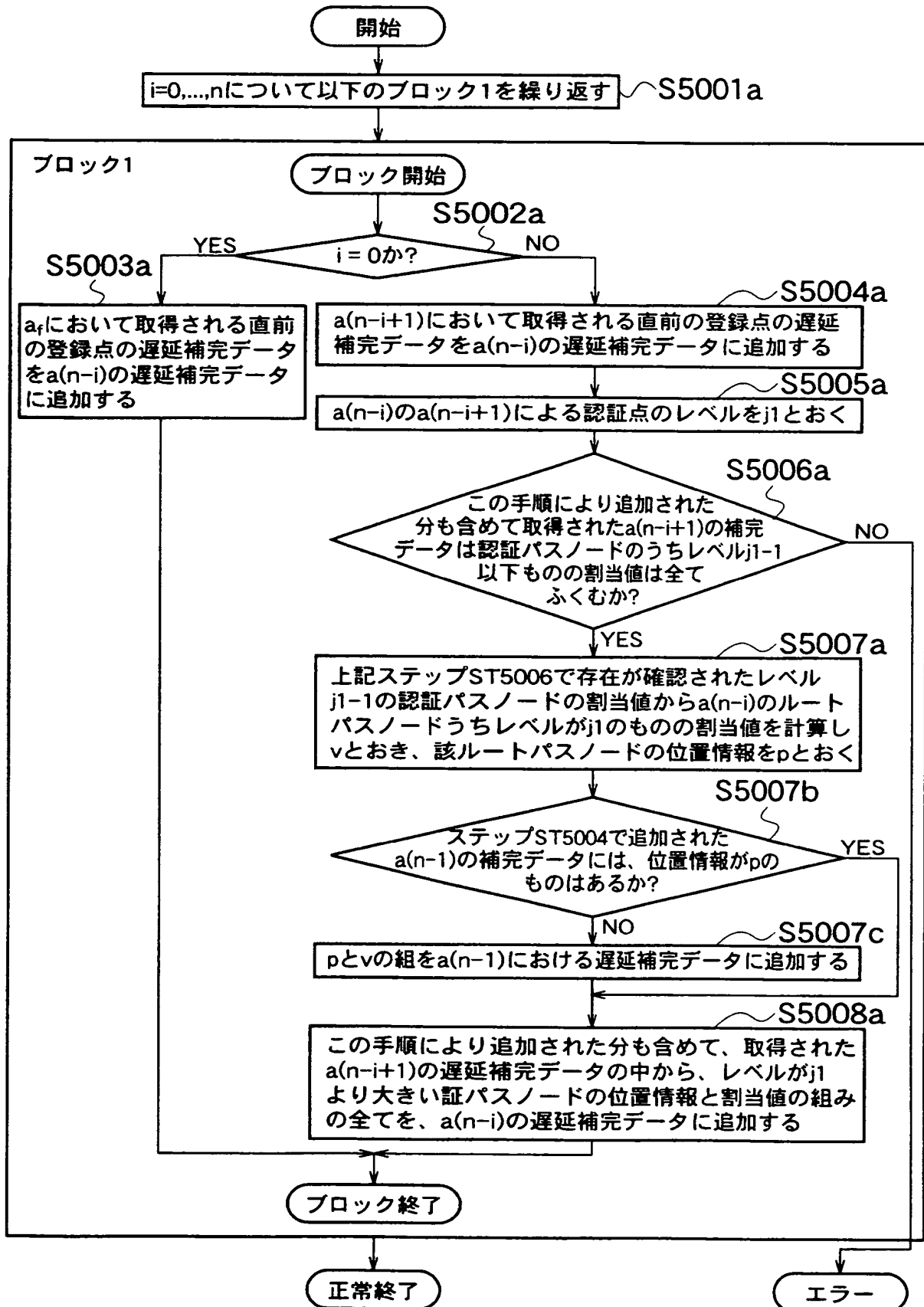
[図66]



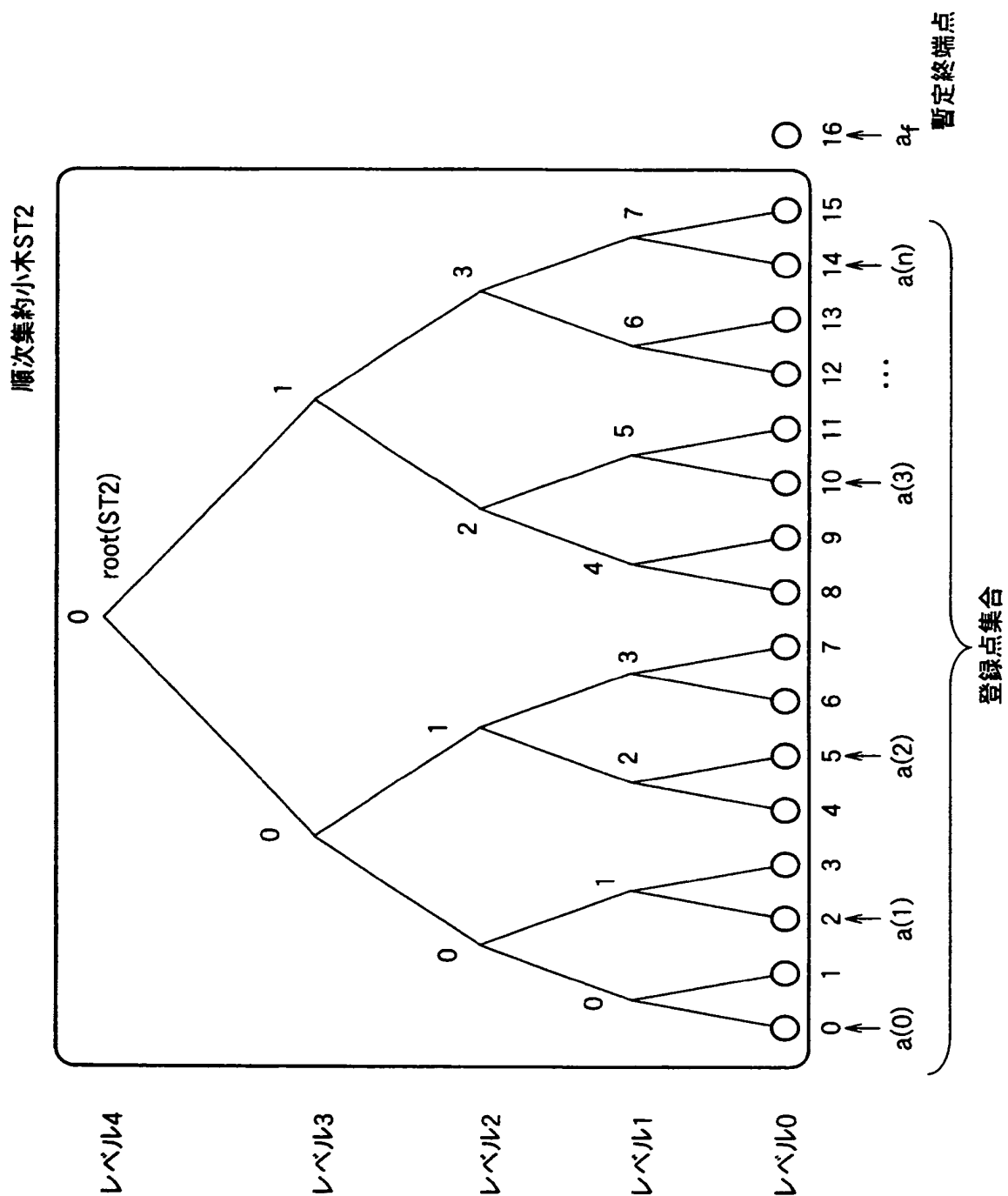
[図67]



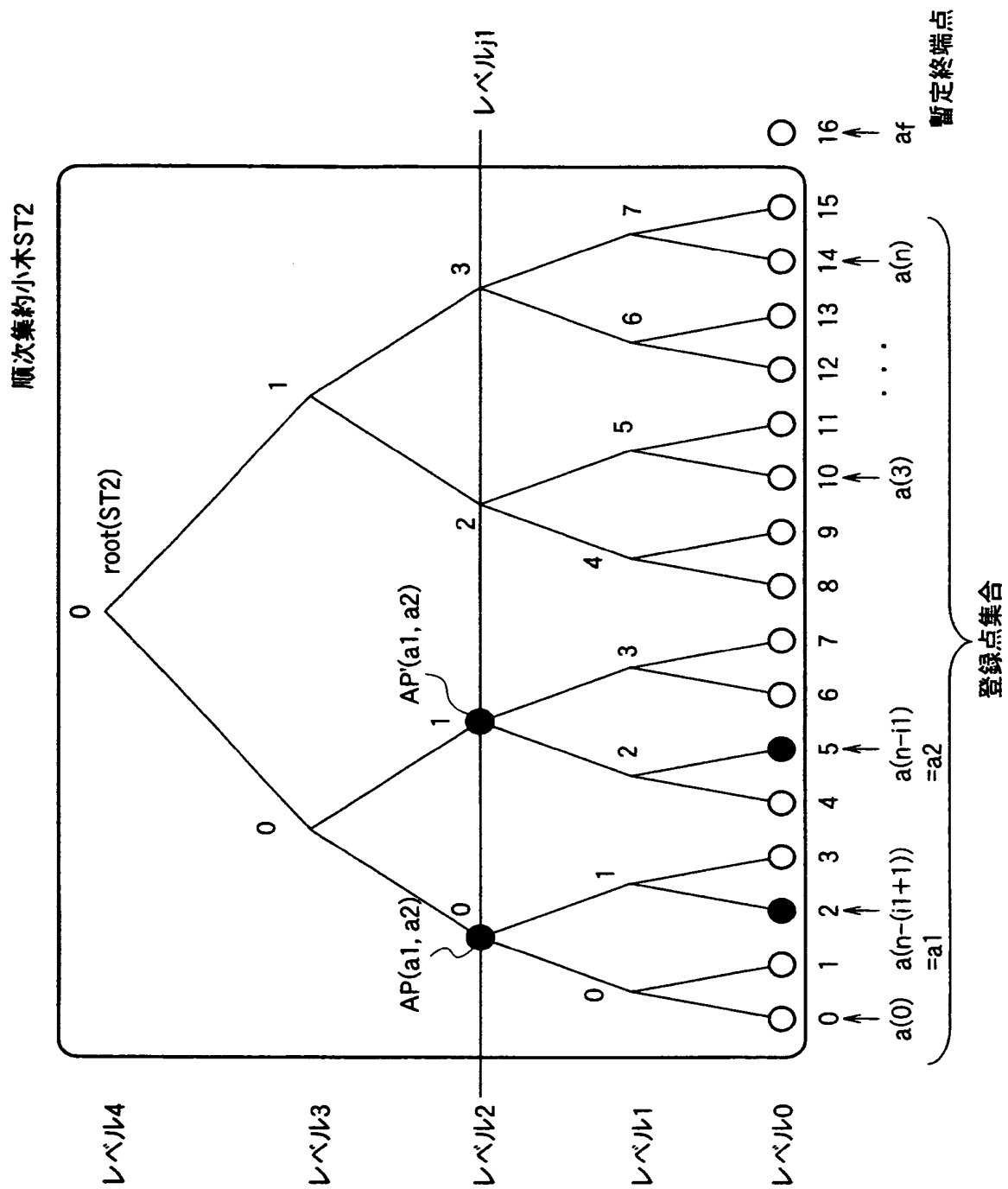
[図68]



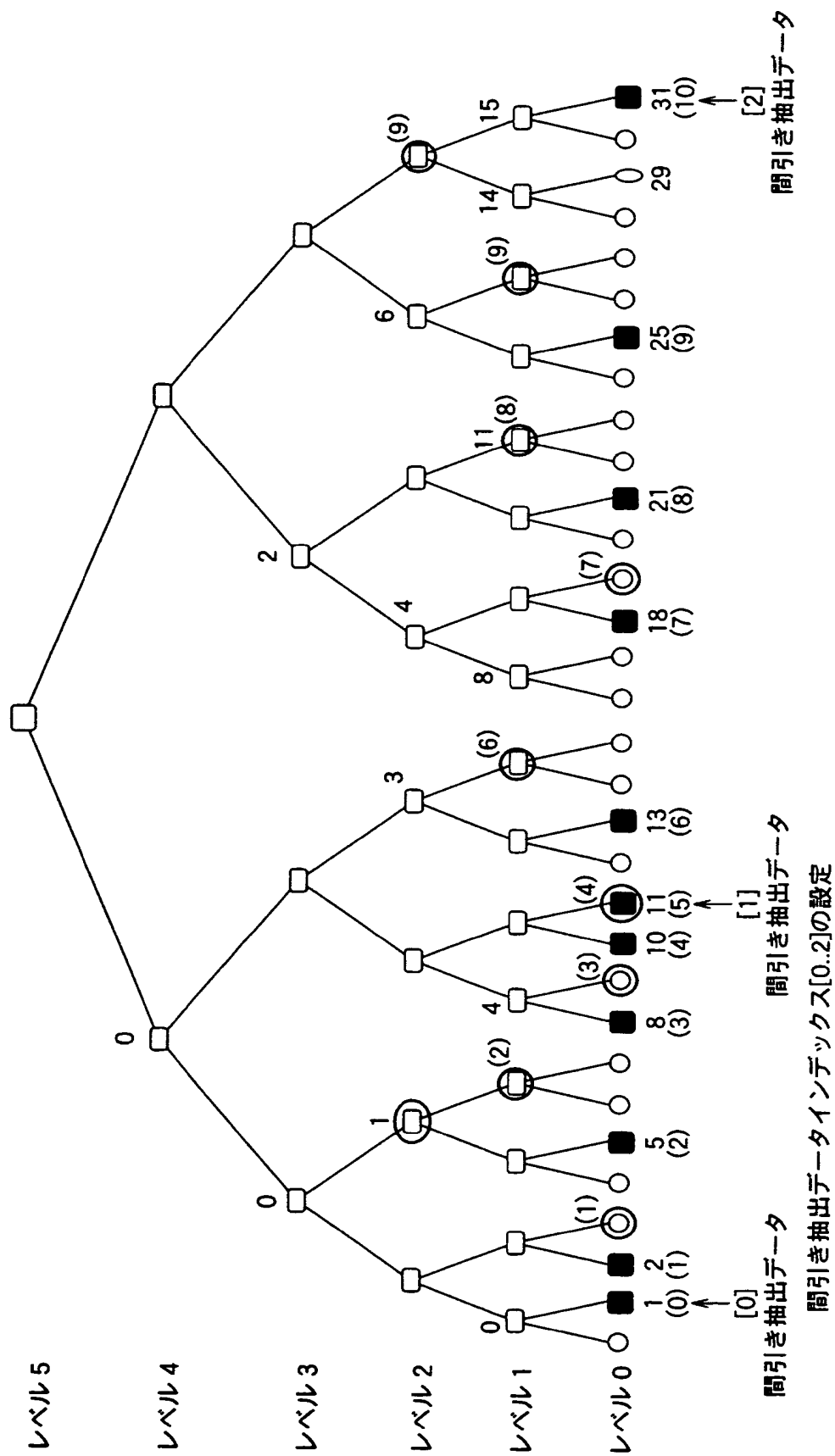
[図69]



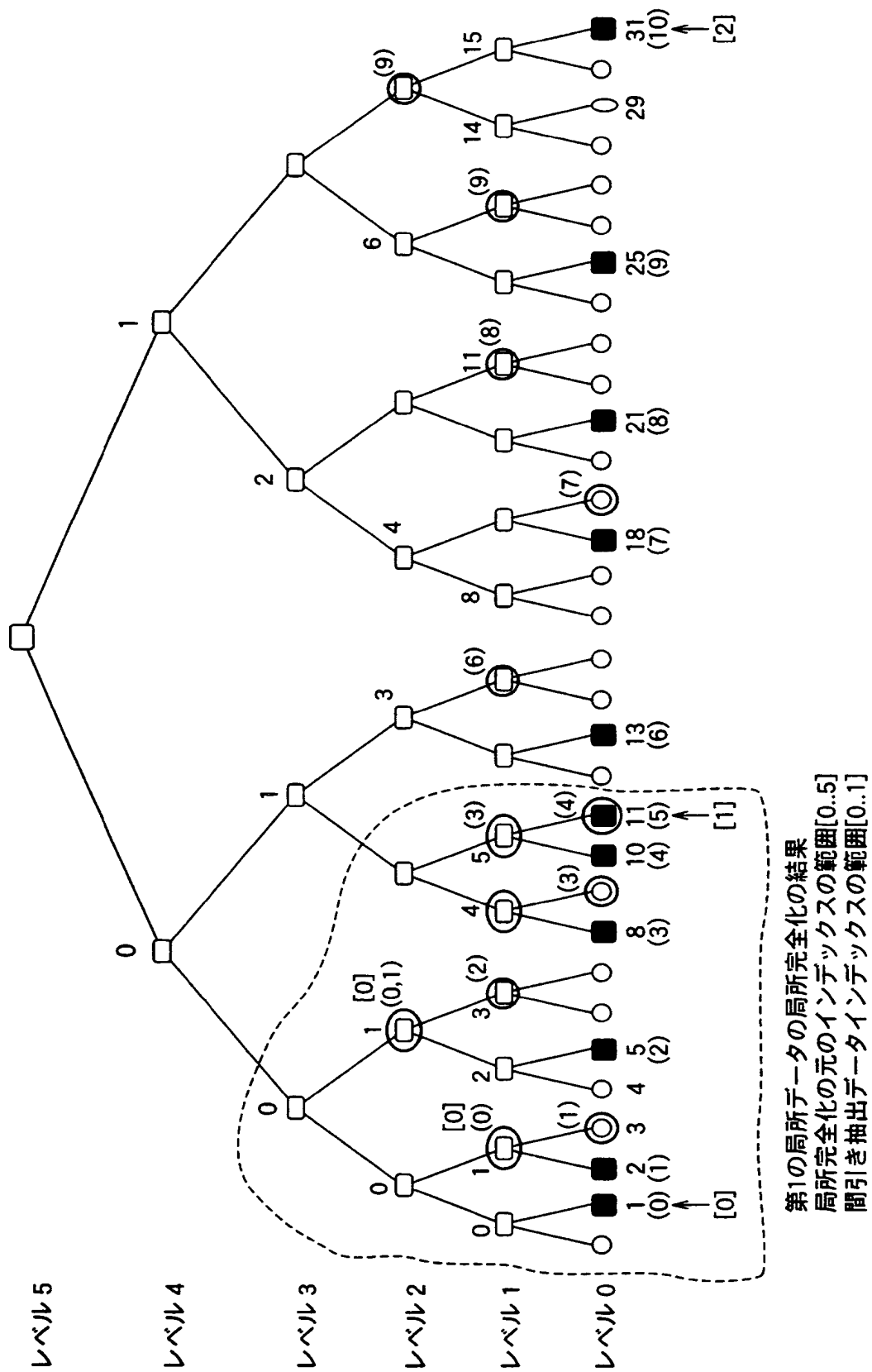
[図70]



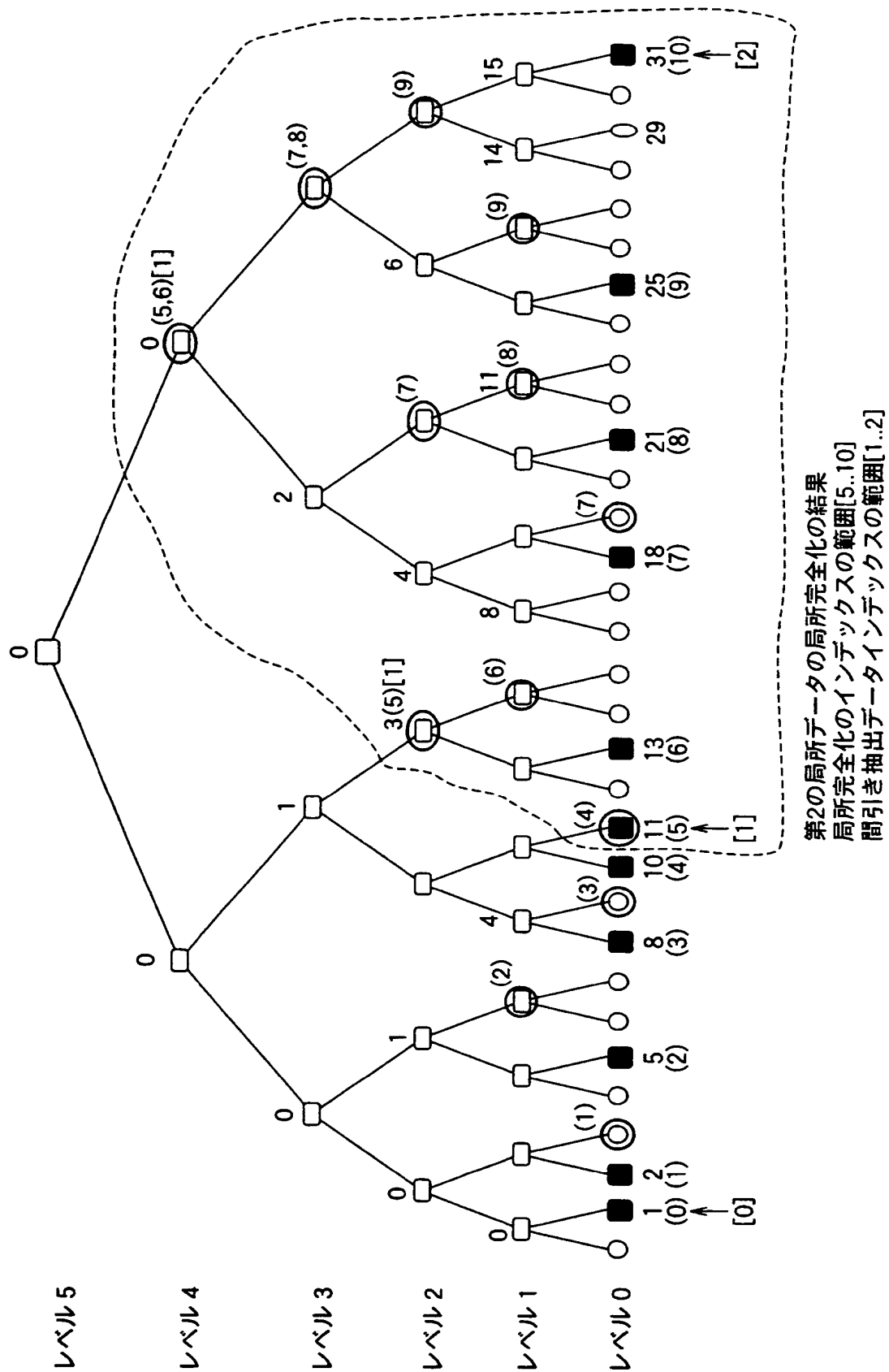
[圖71]



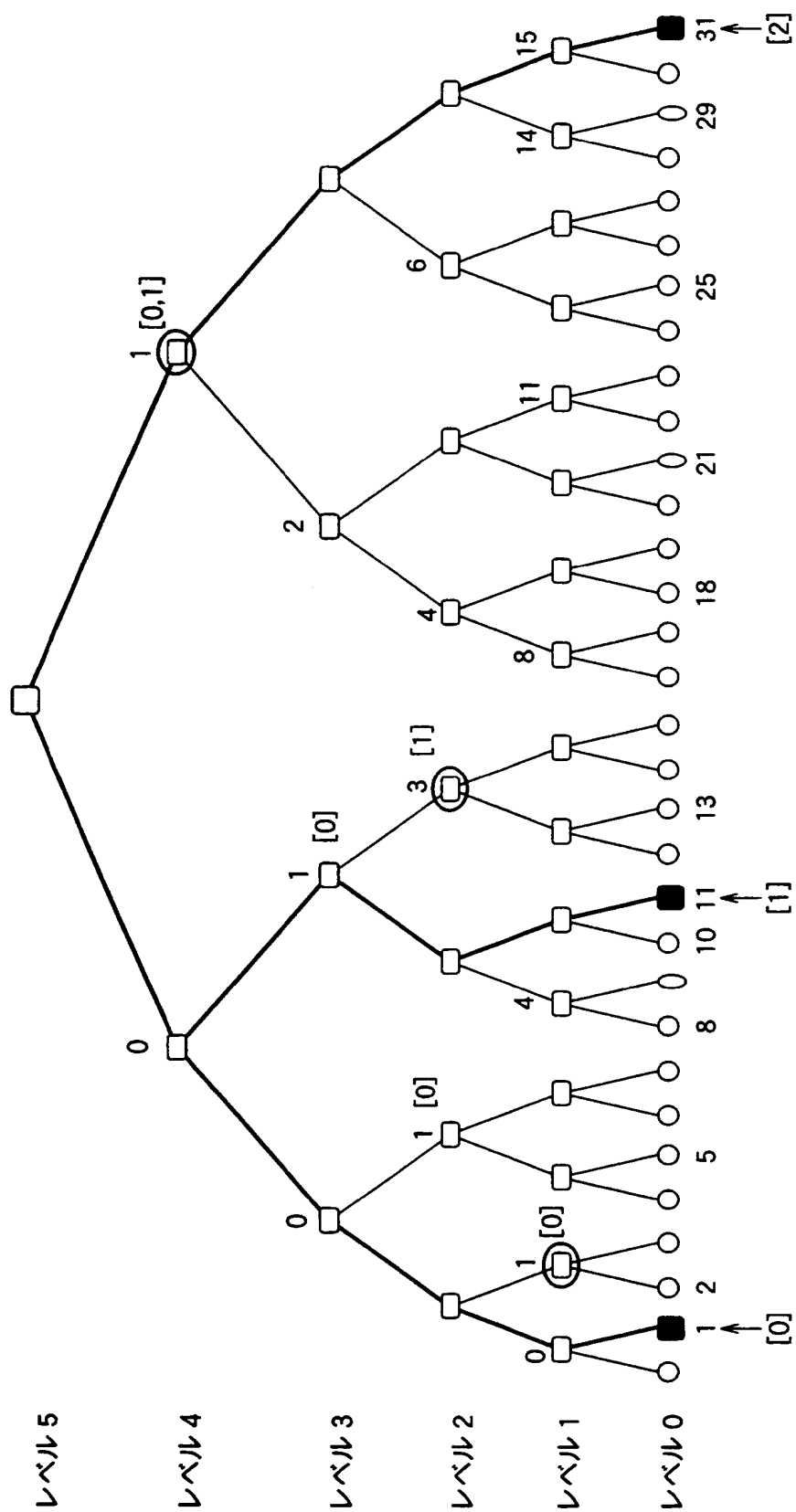
[図72]



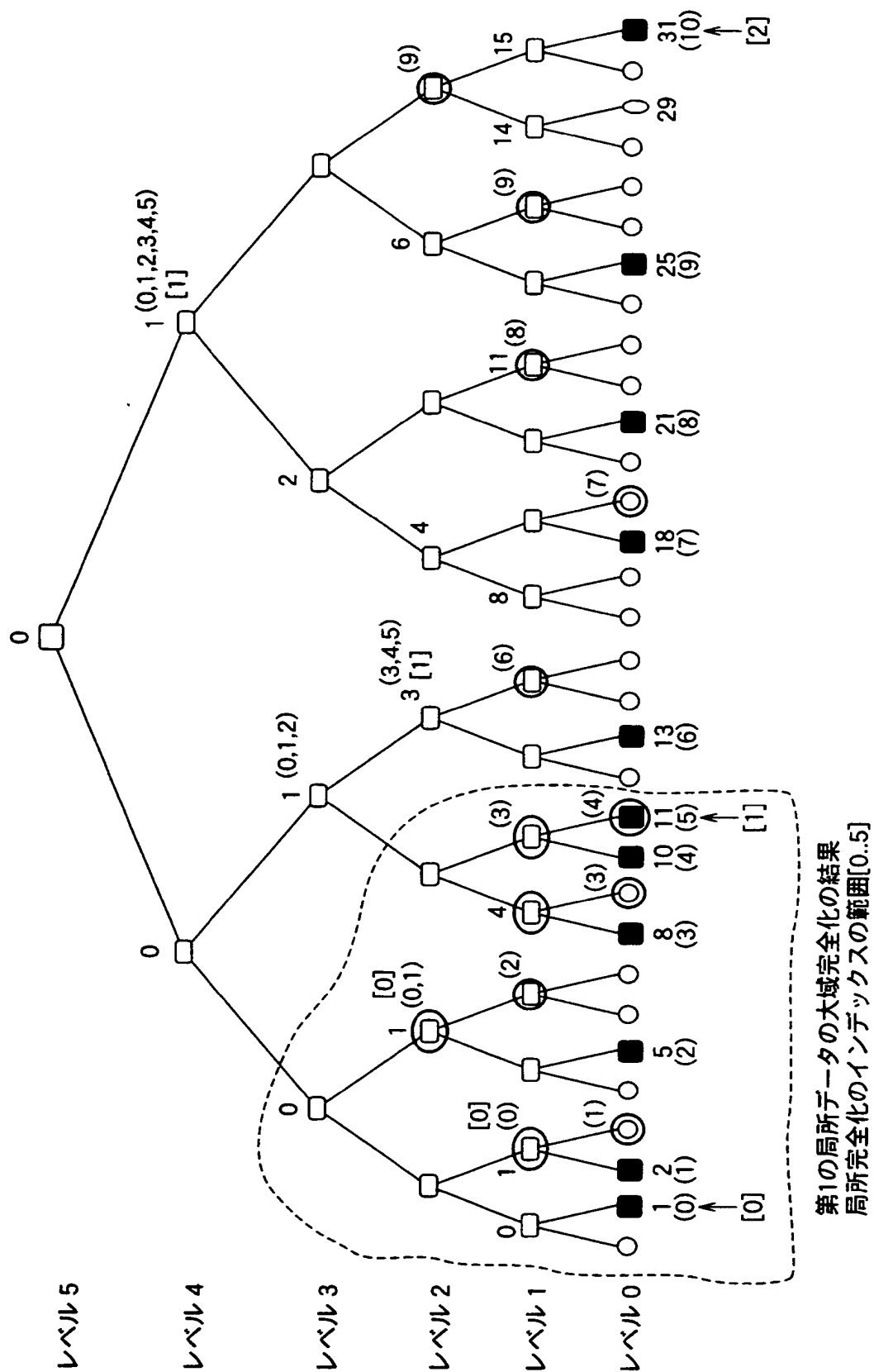
[図73]



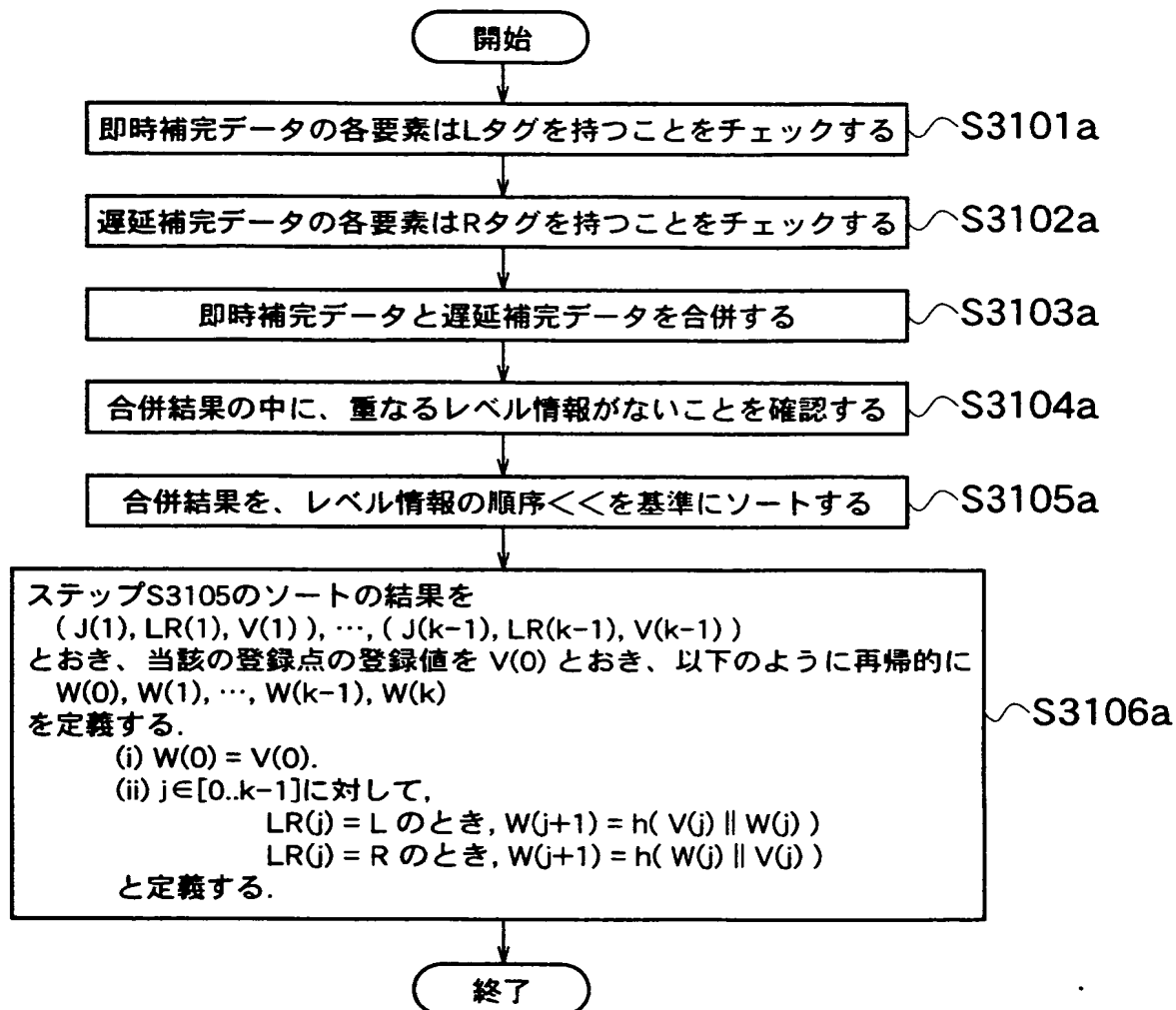
[図74]



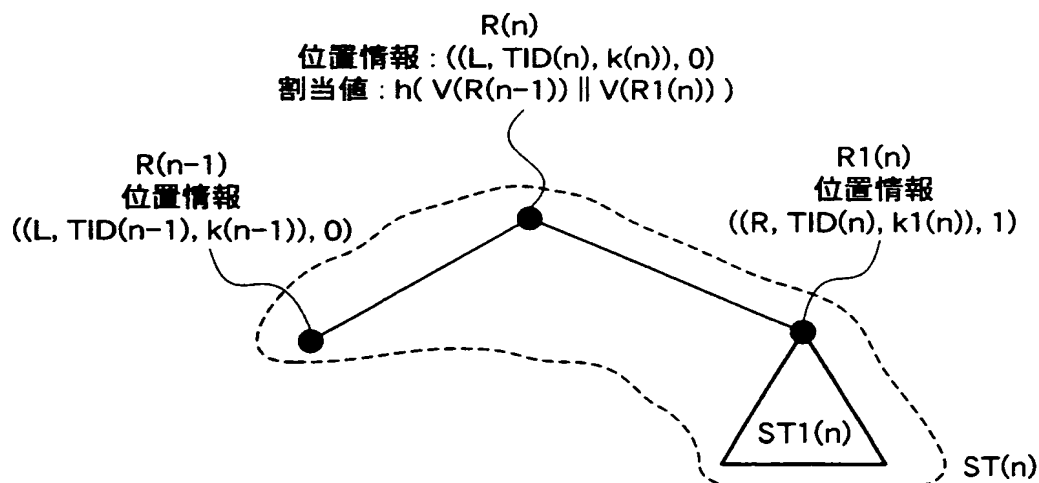
[図75]



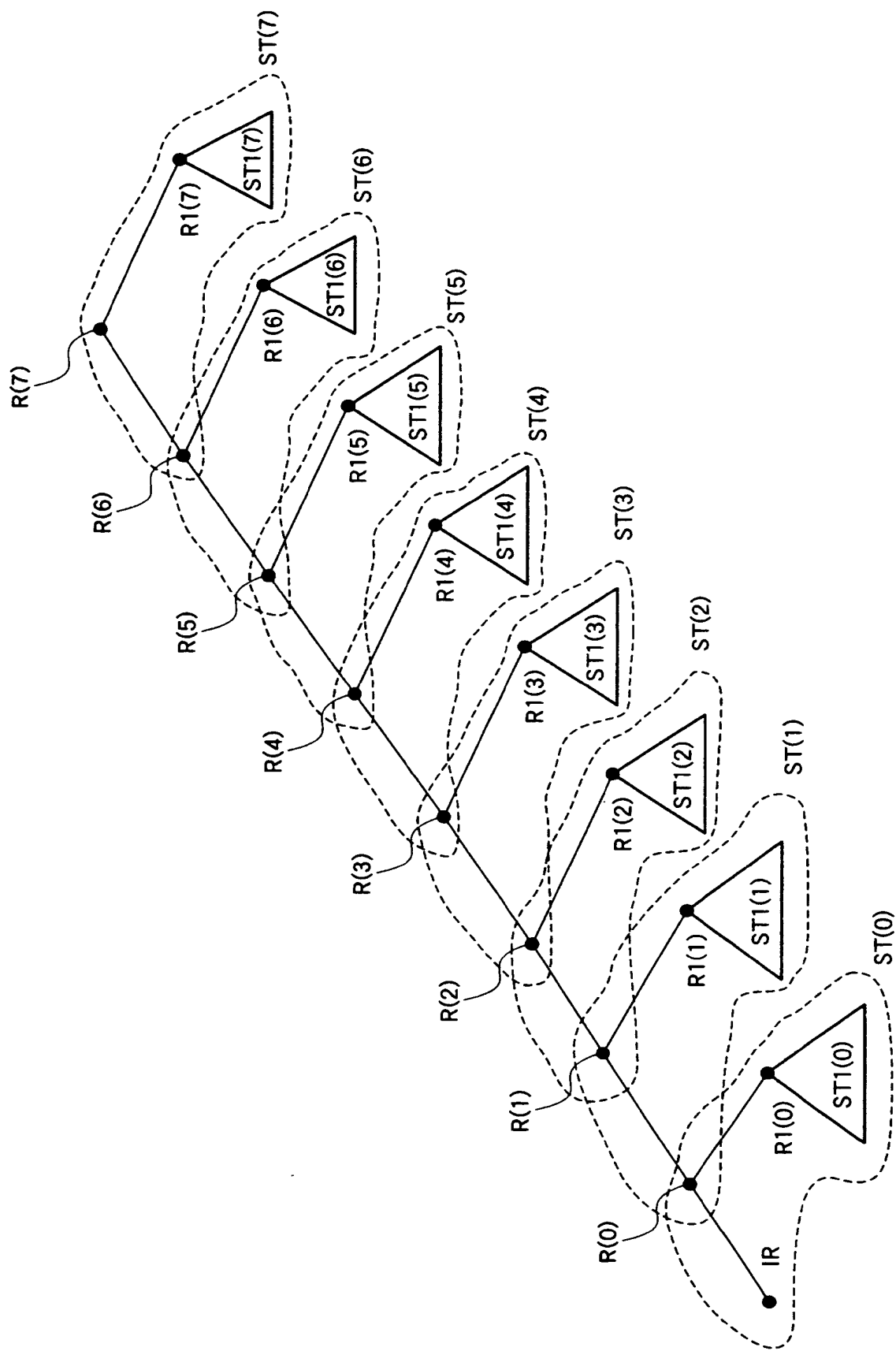
[図76]



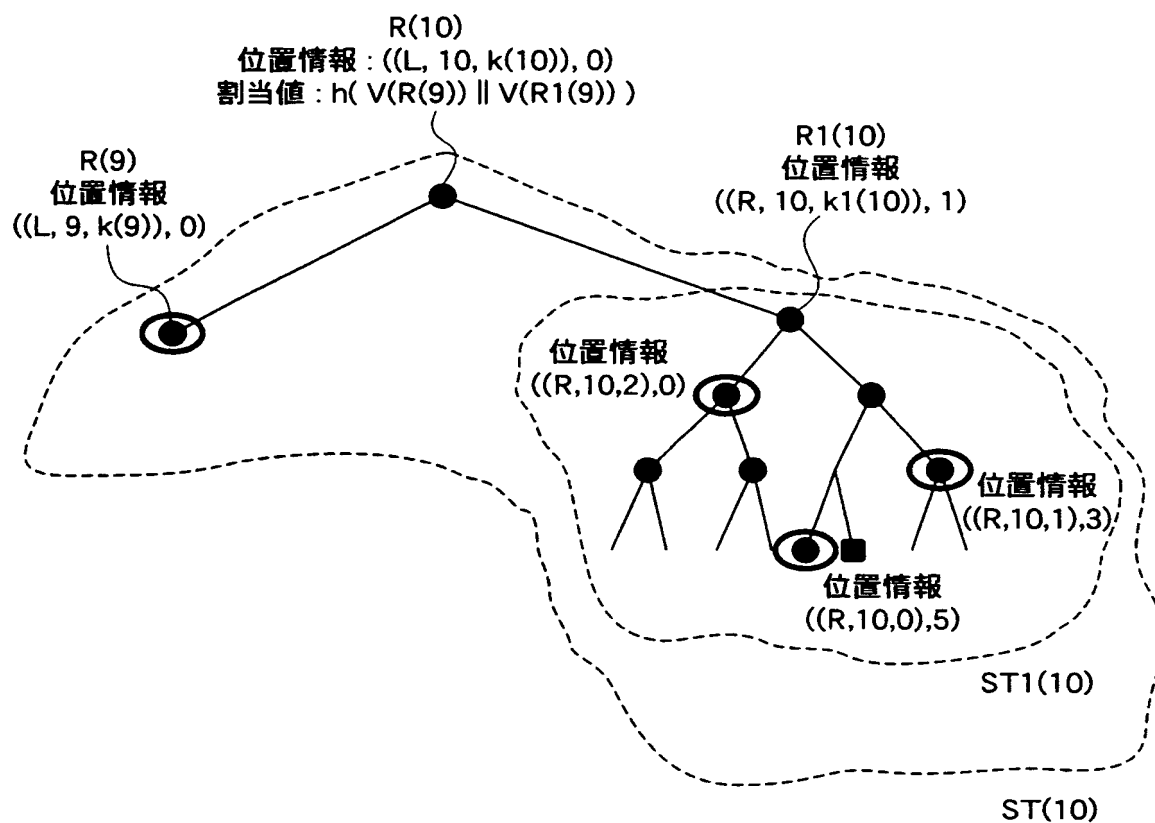
[図77]



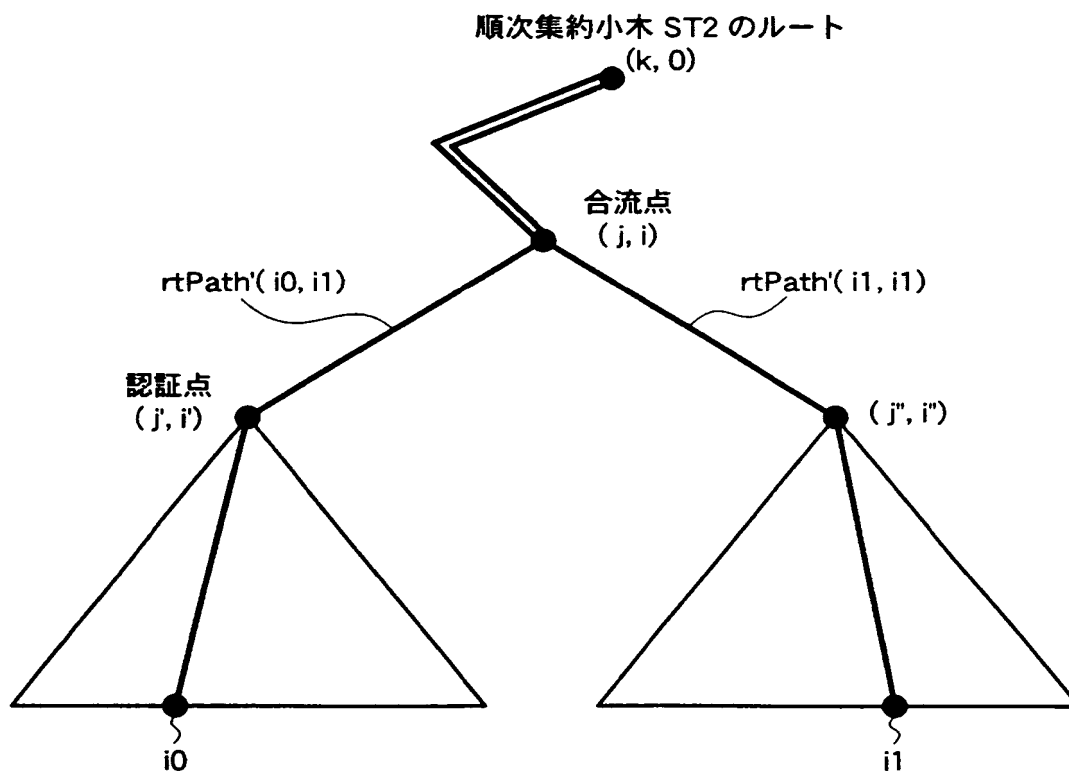
[図78]



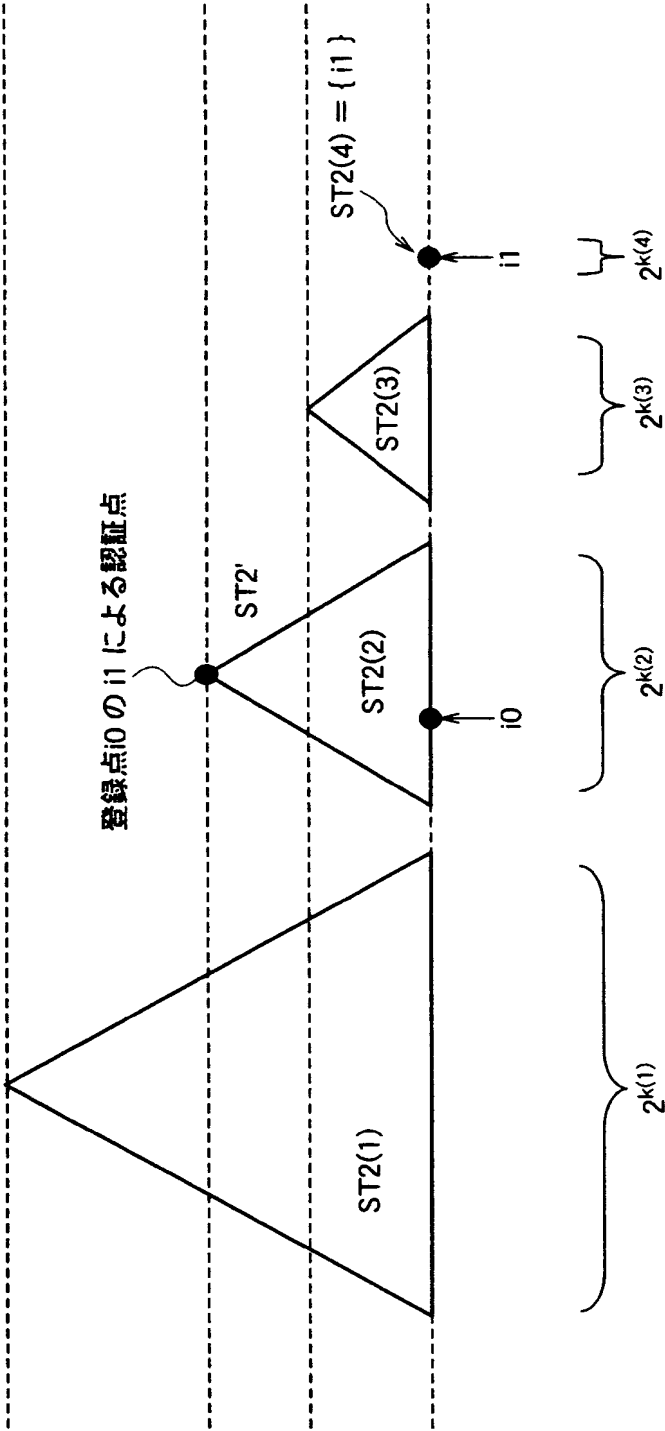
[図79]



[図80]

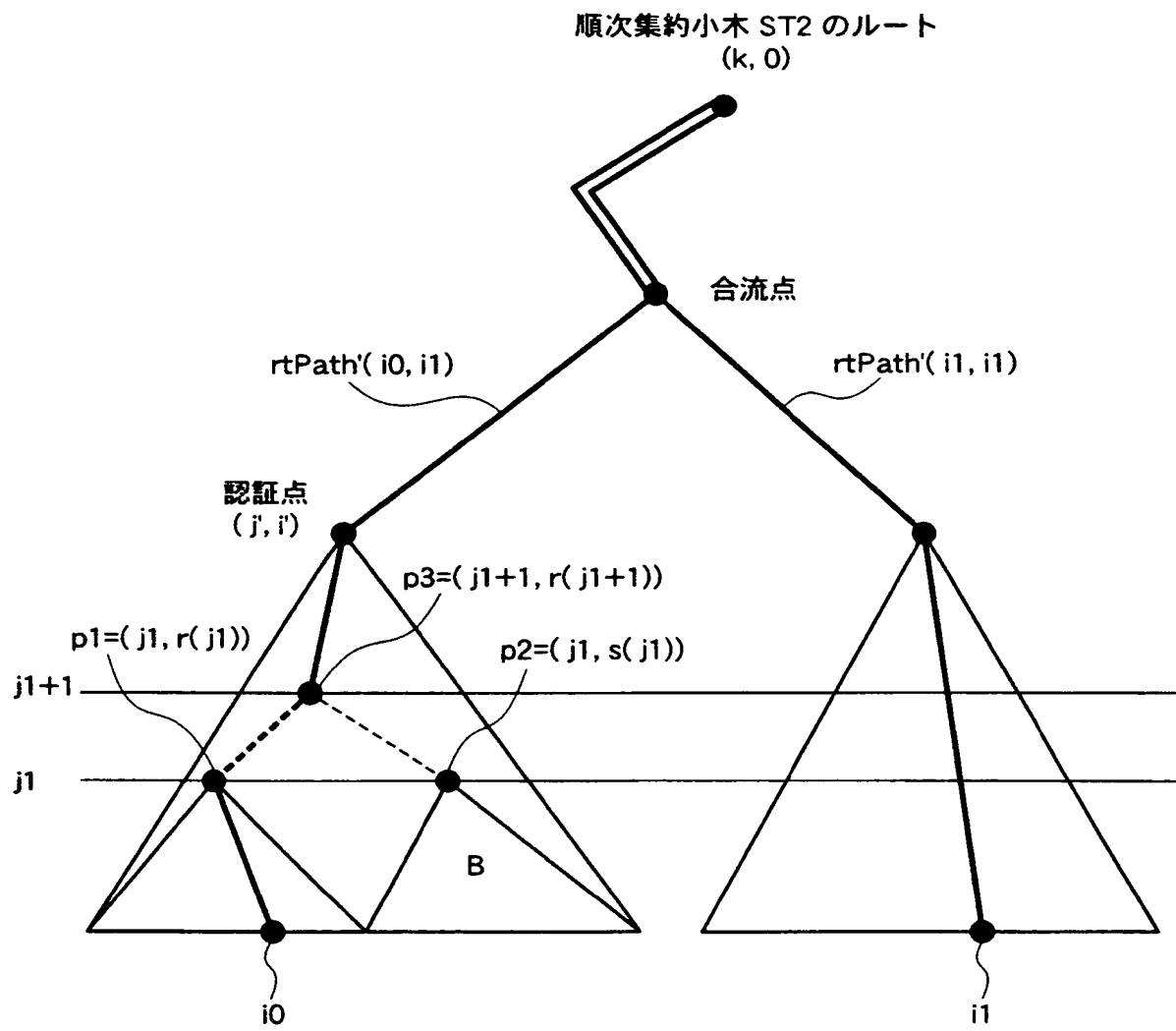


[図81]

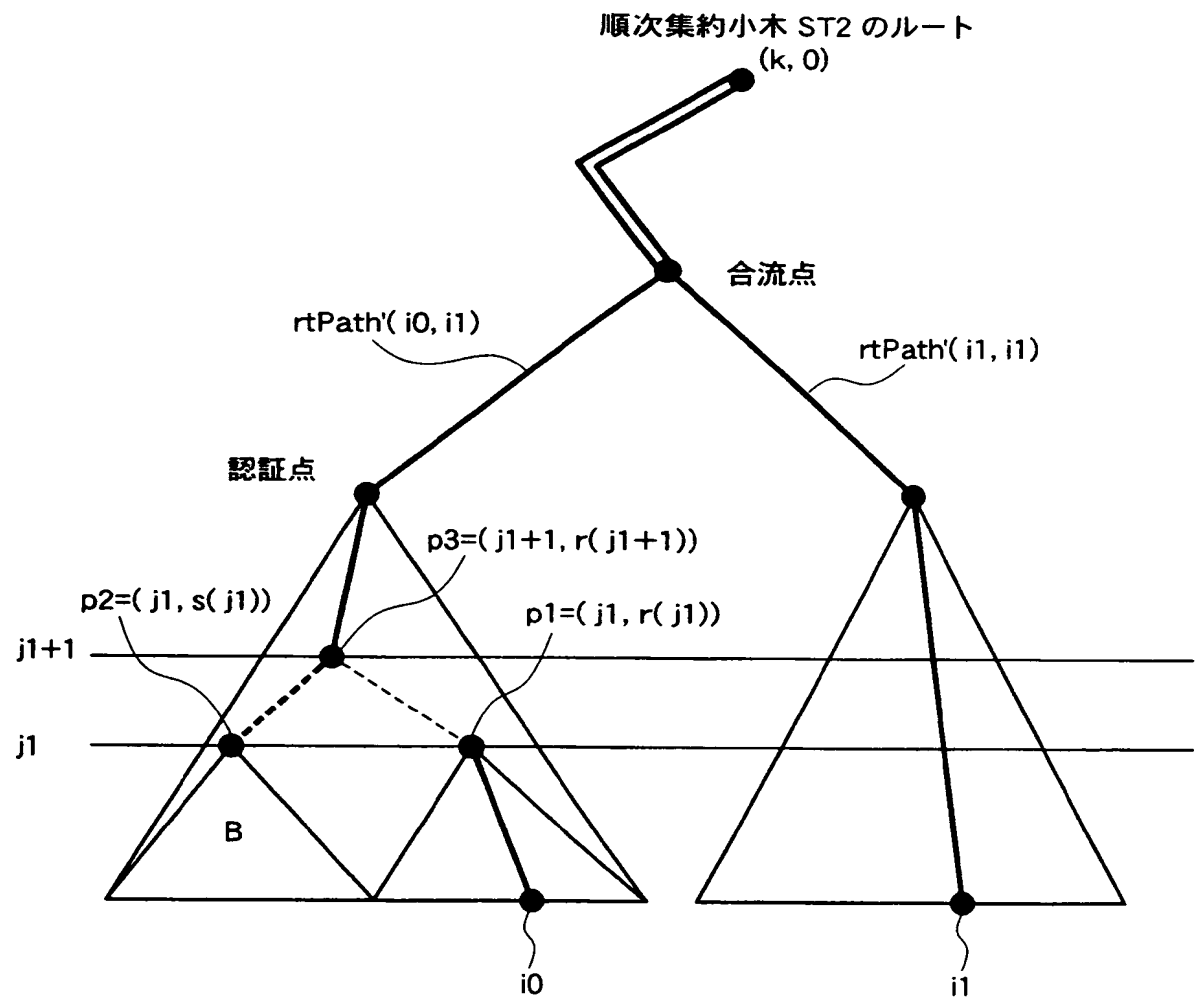


$k(1) > k(2) > k(3) > k(4) = 0$

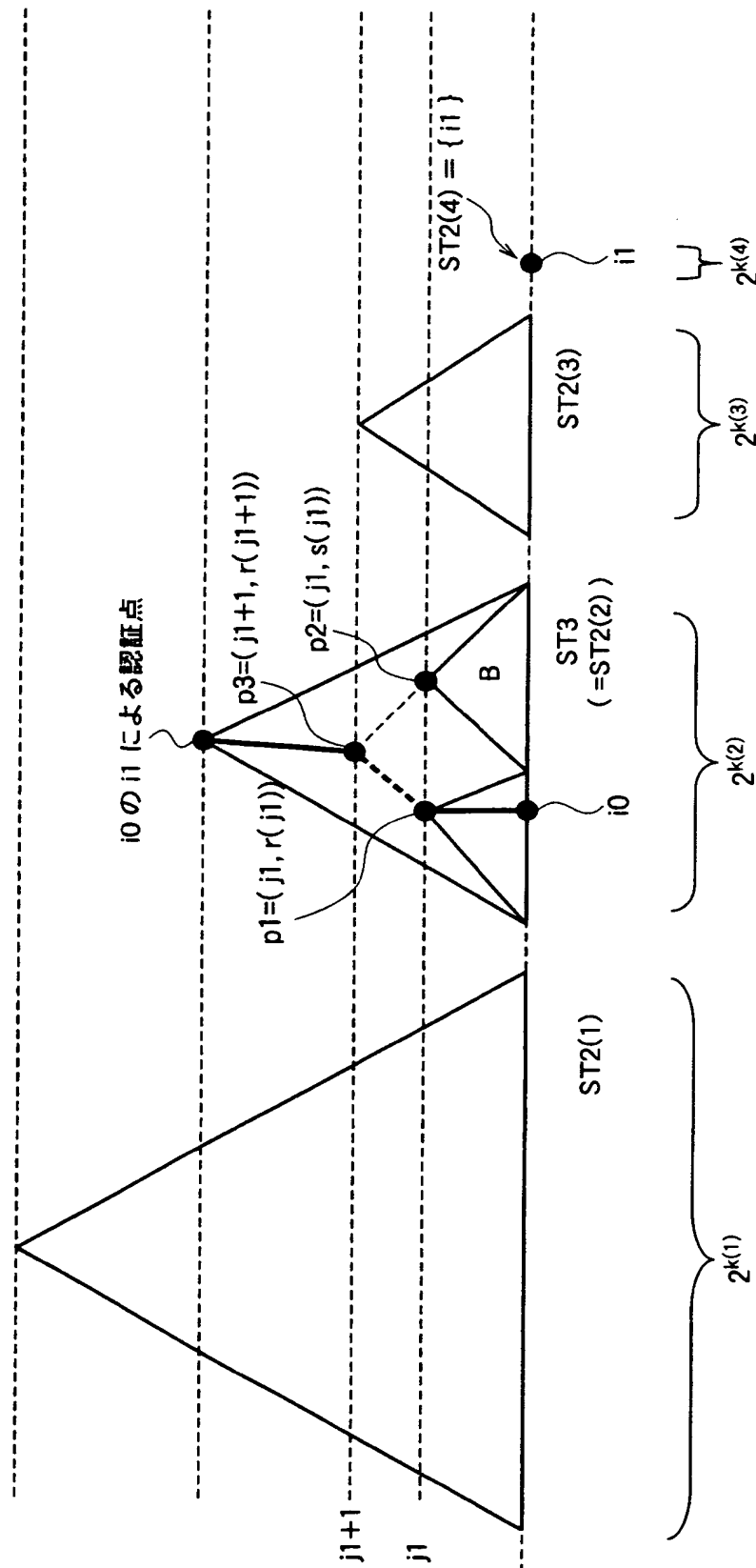
[図82]



[図83]

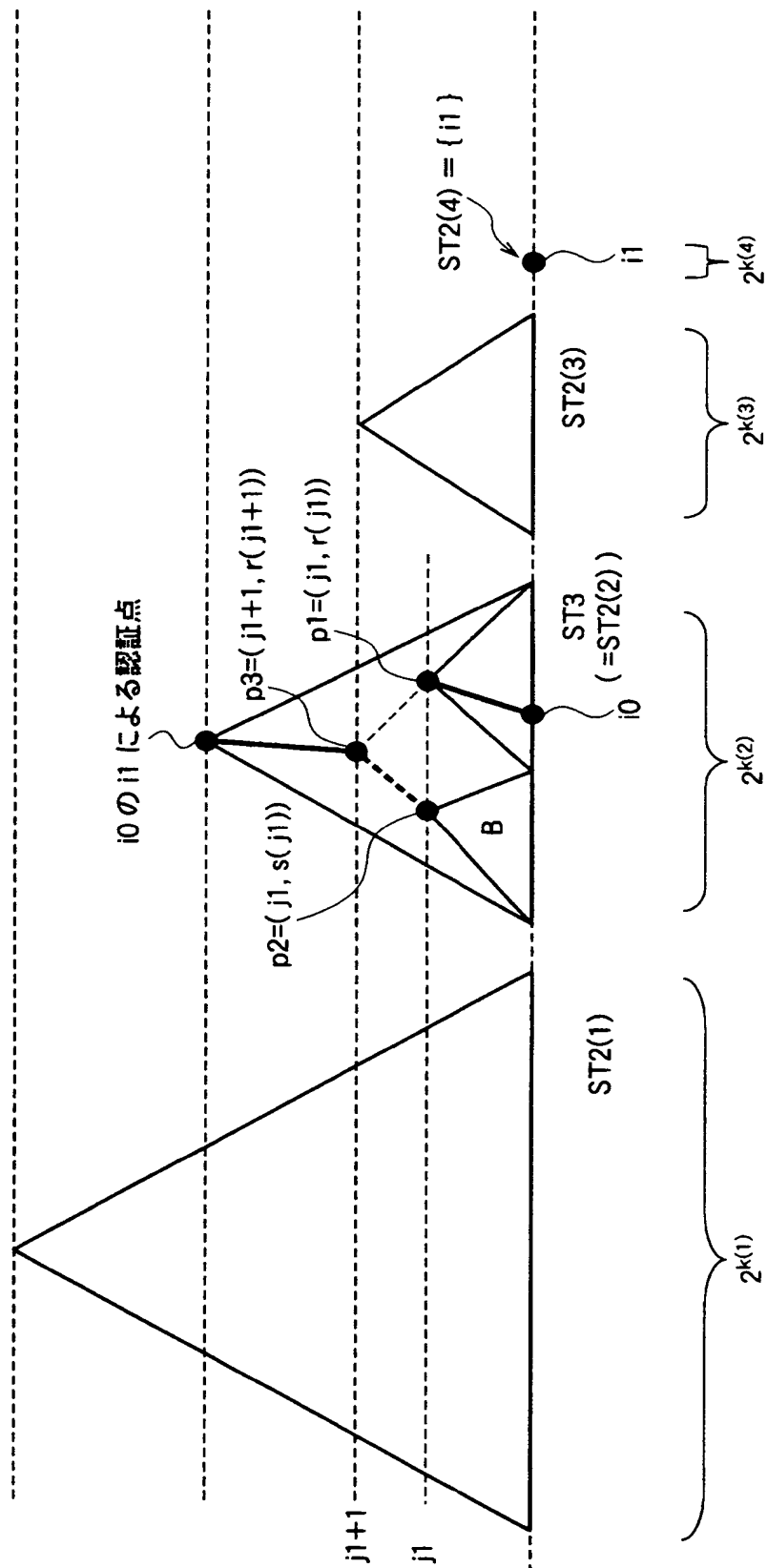


[図84]



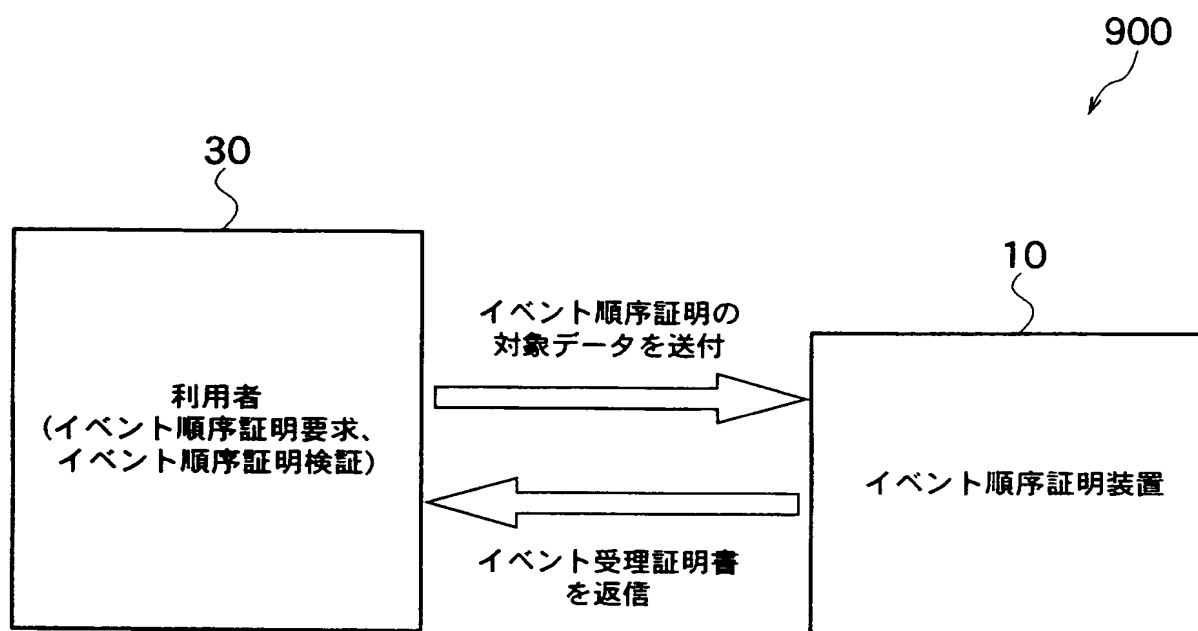
$$k(1) > k(2) > k(3) > k(4) = 0$$

[図85]

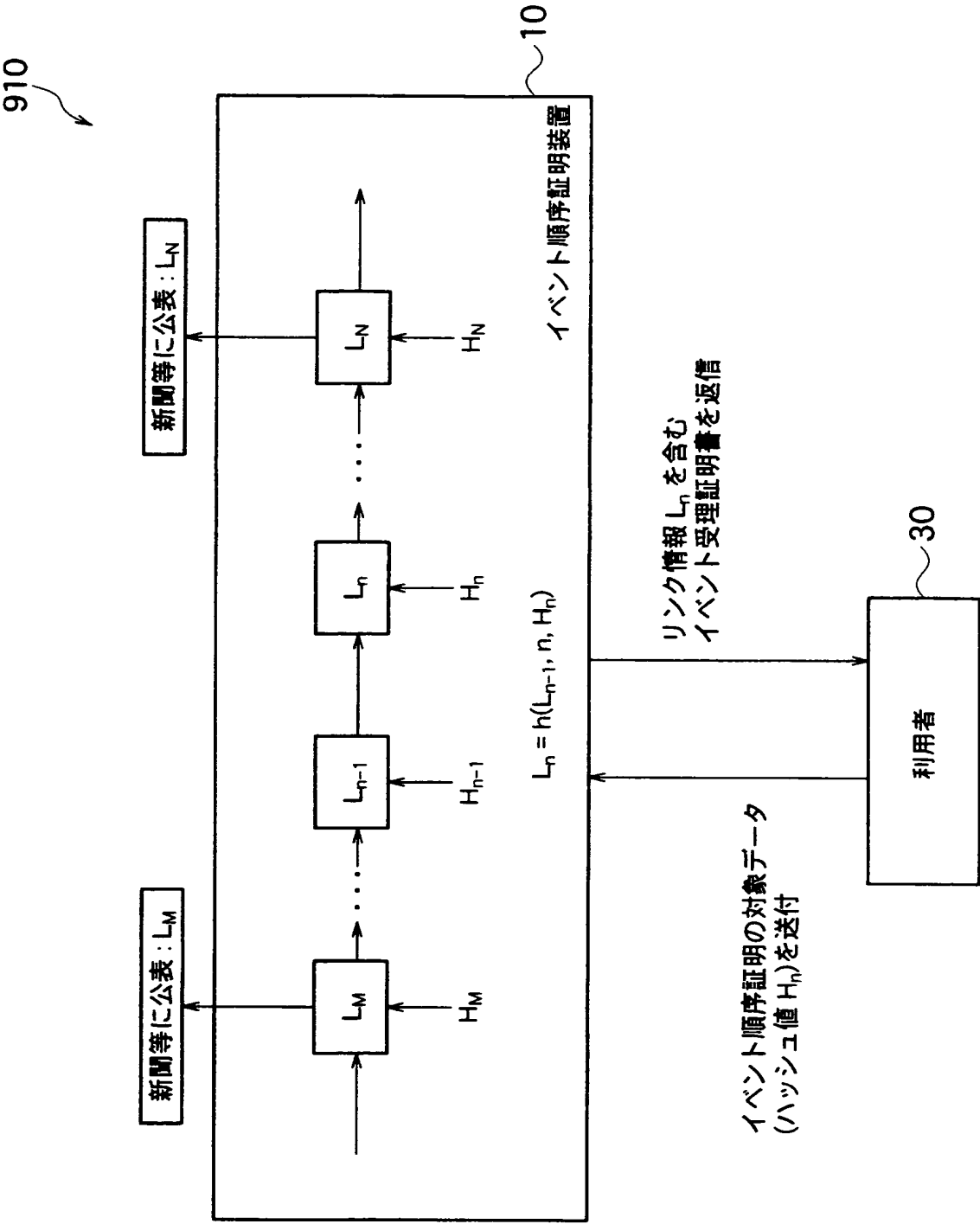


$$k(1) > k(2) > k(3) > k(4) = 0$$

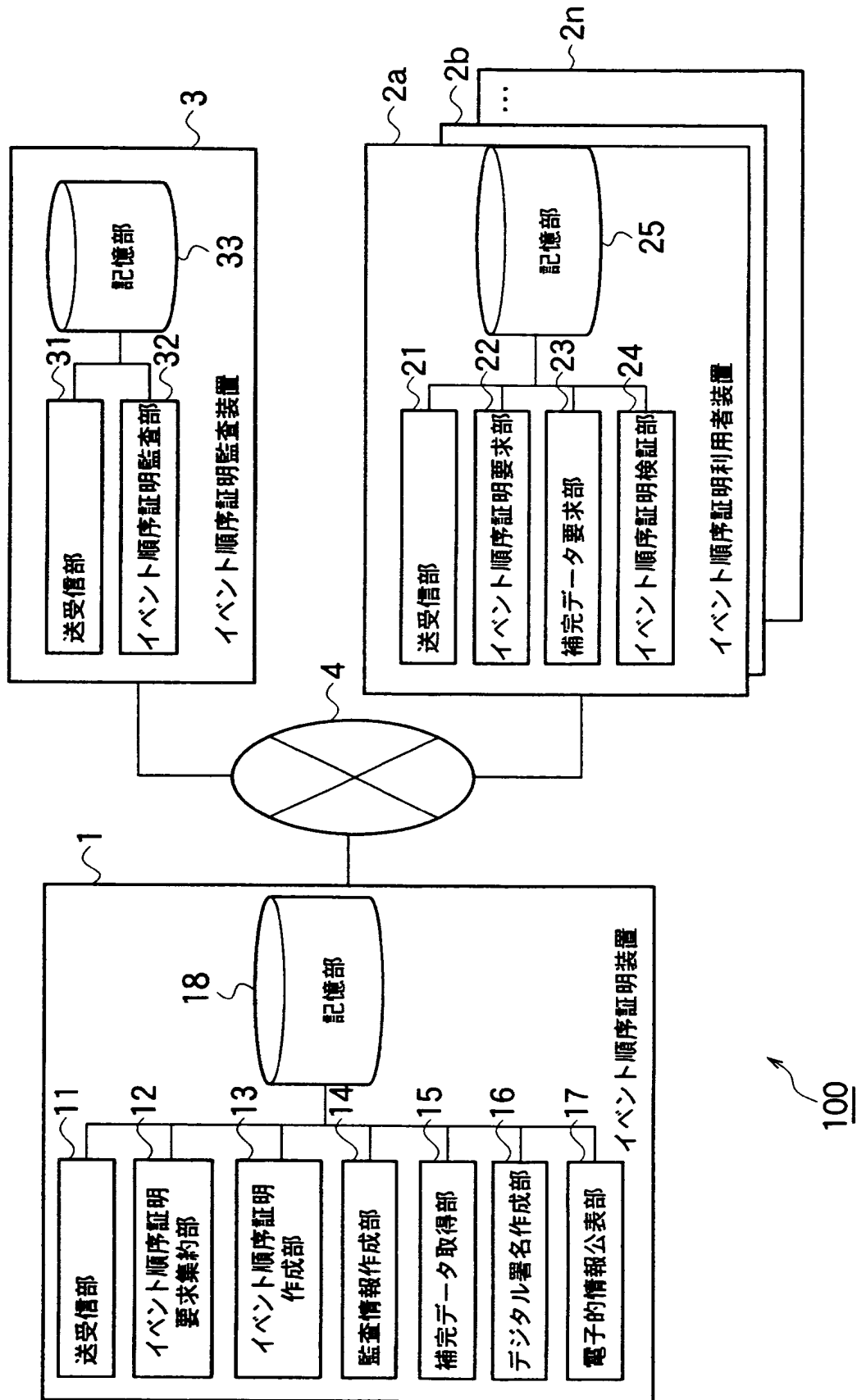
[図1]



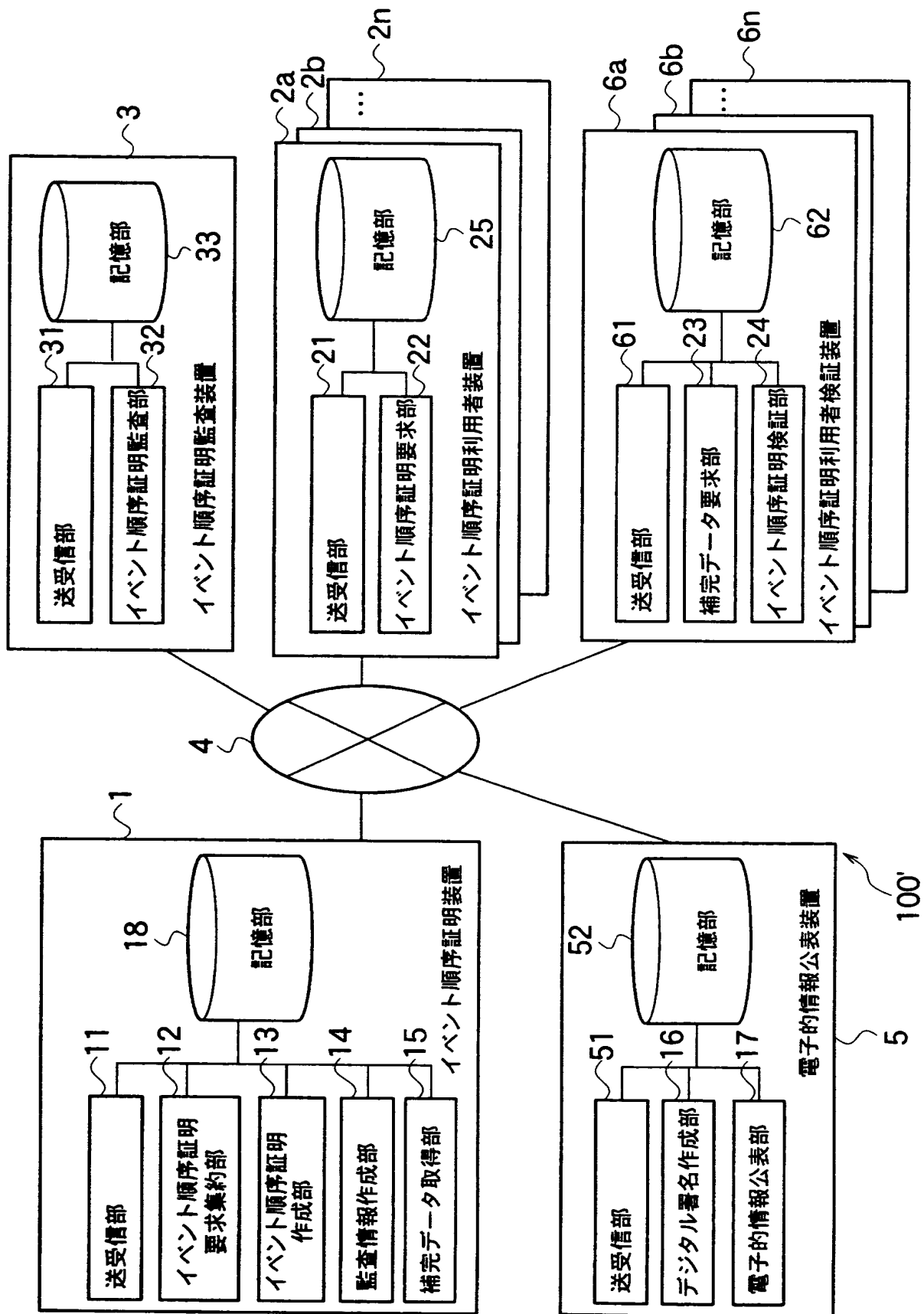
[図2]



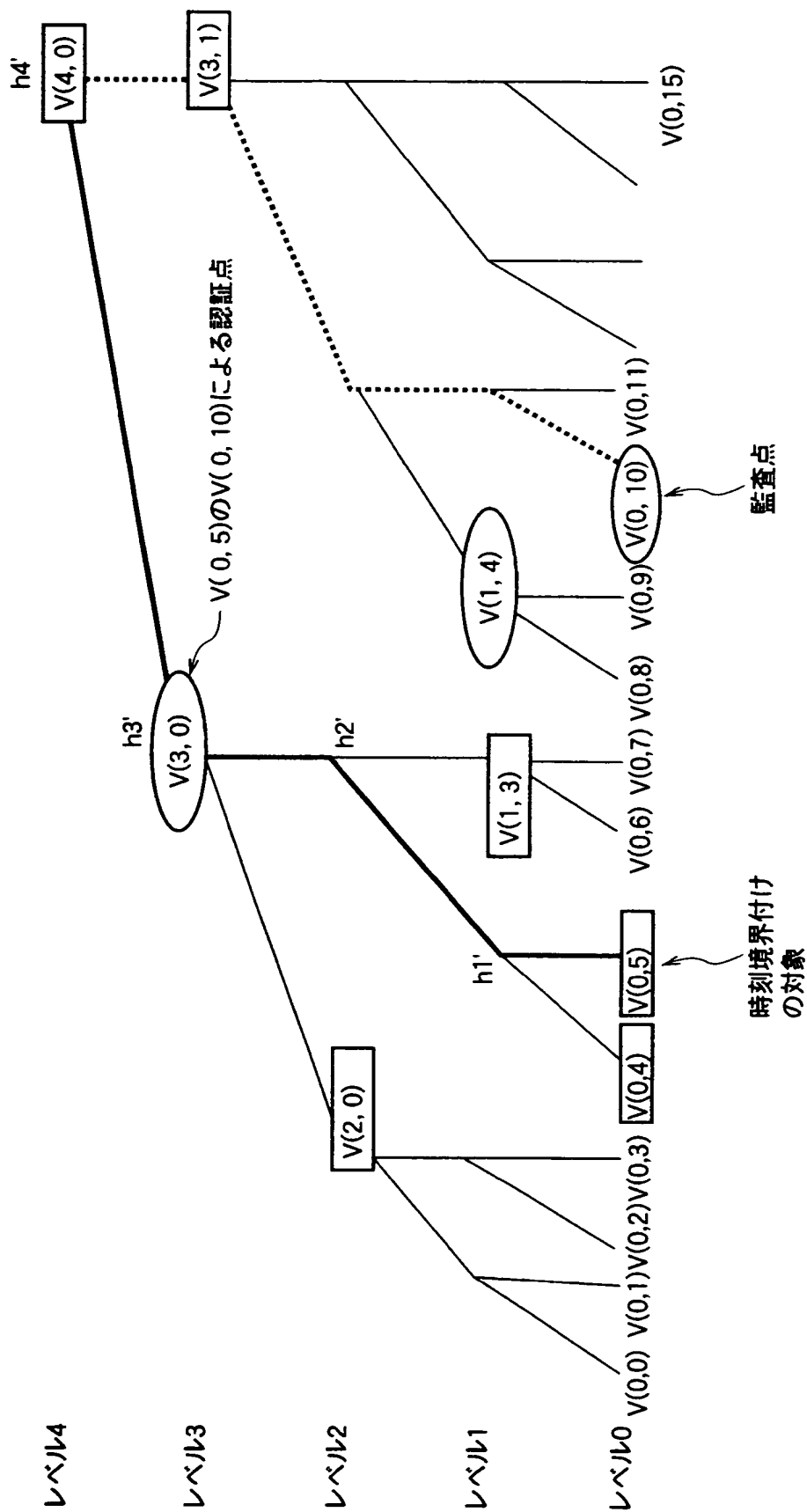
[図3]



[図4]



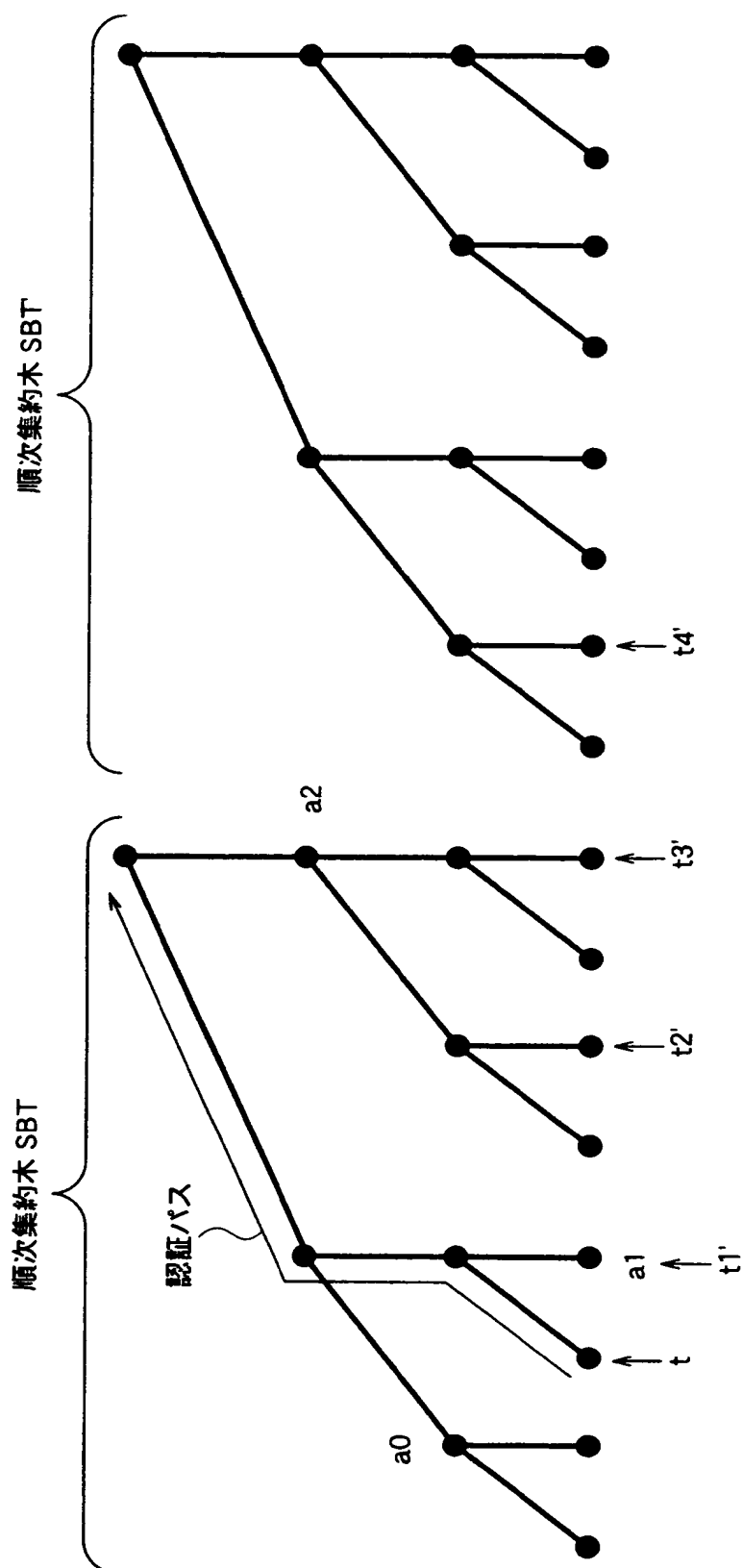
[図5]



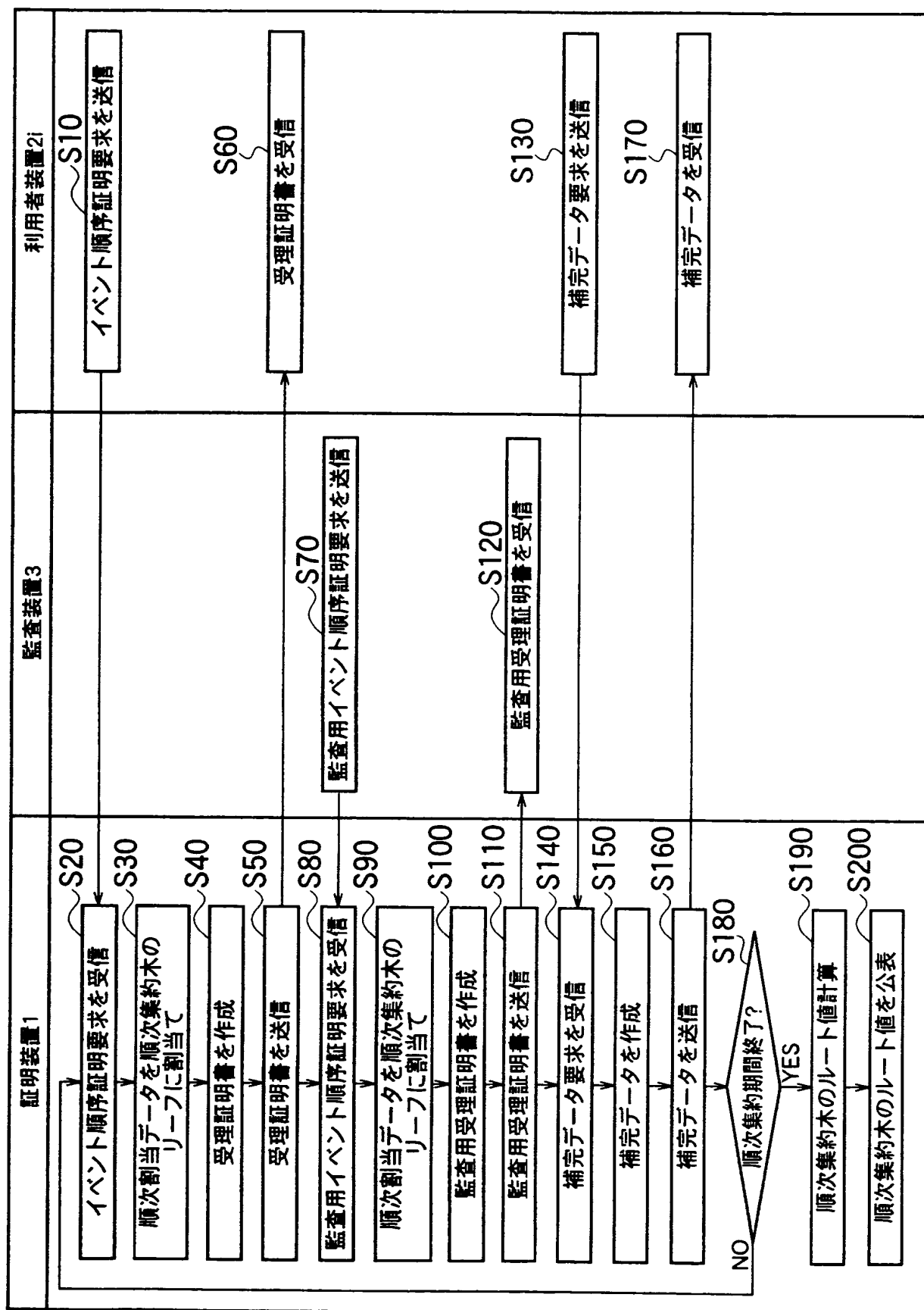
[図6]

項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木番号	n	○
順次集約木リーフ番号	i	○
即時補完データ(位置情報、割当値)	HK	
デジタル署名	DS	

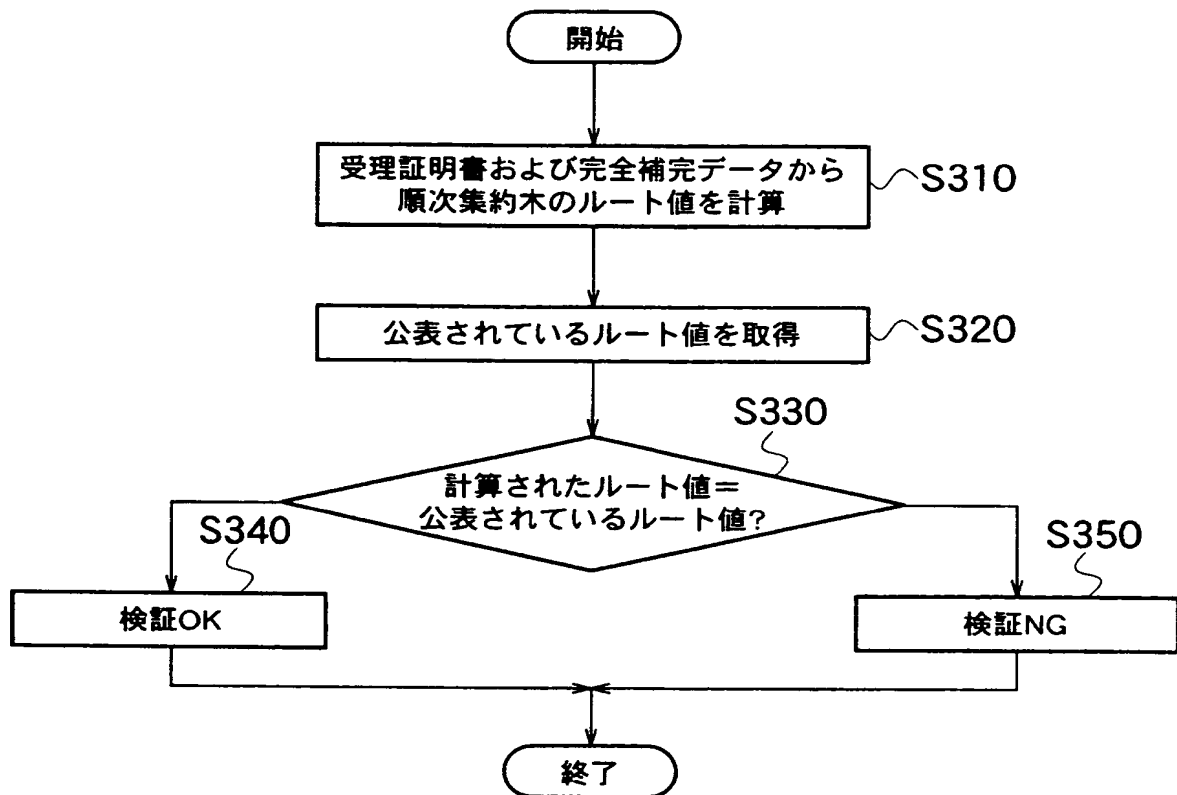
[図7]



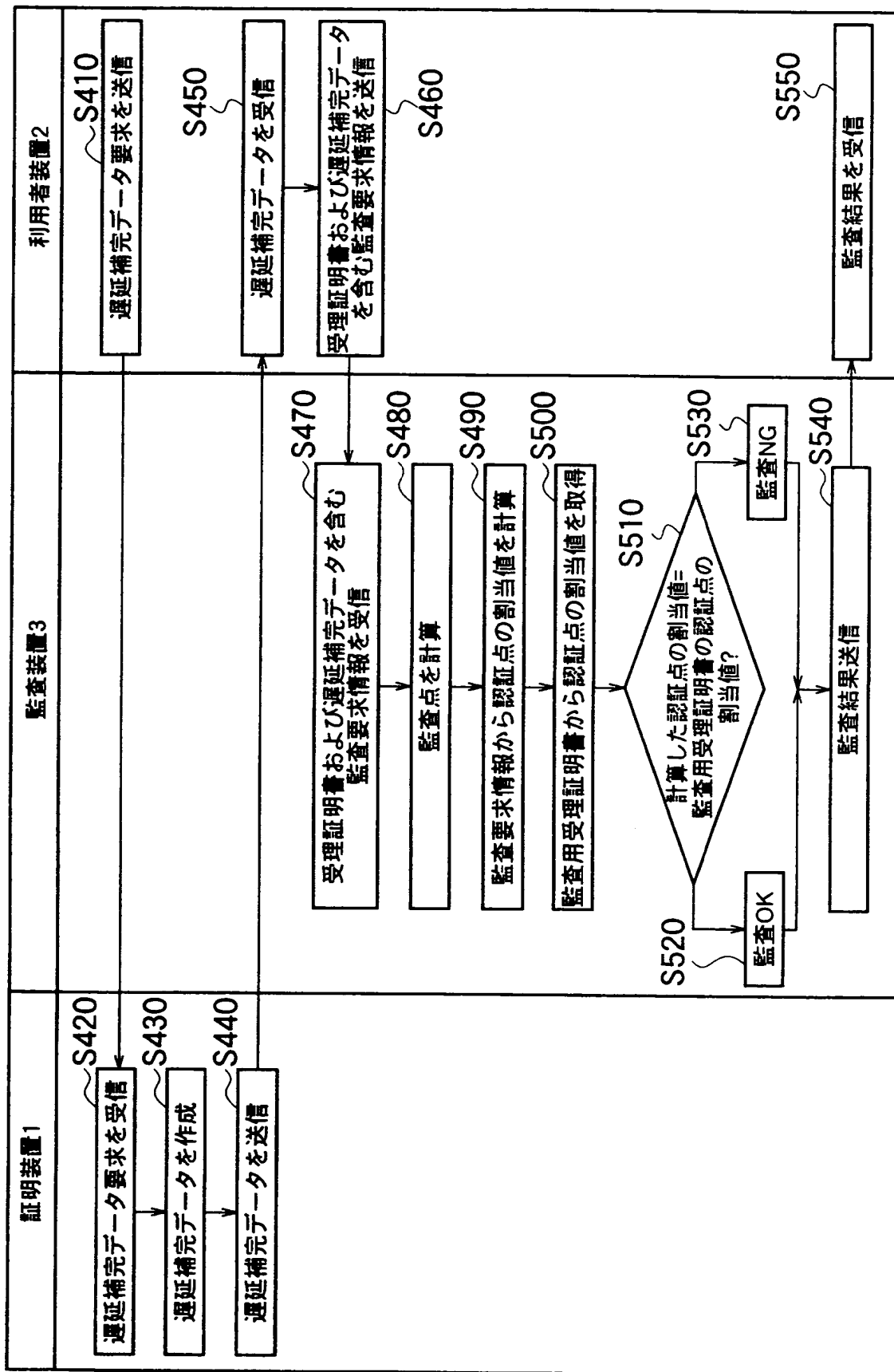
[図8]



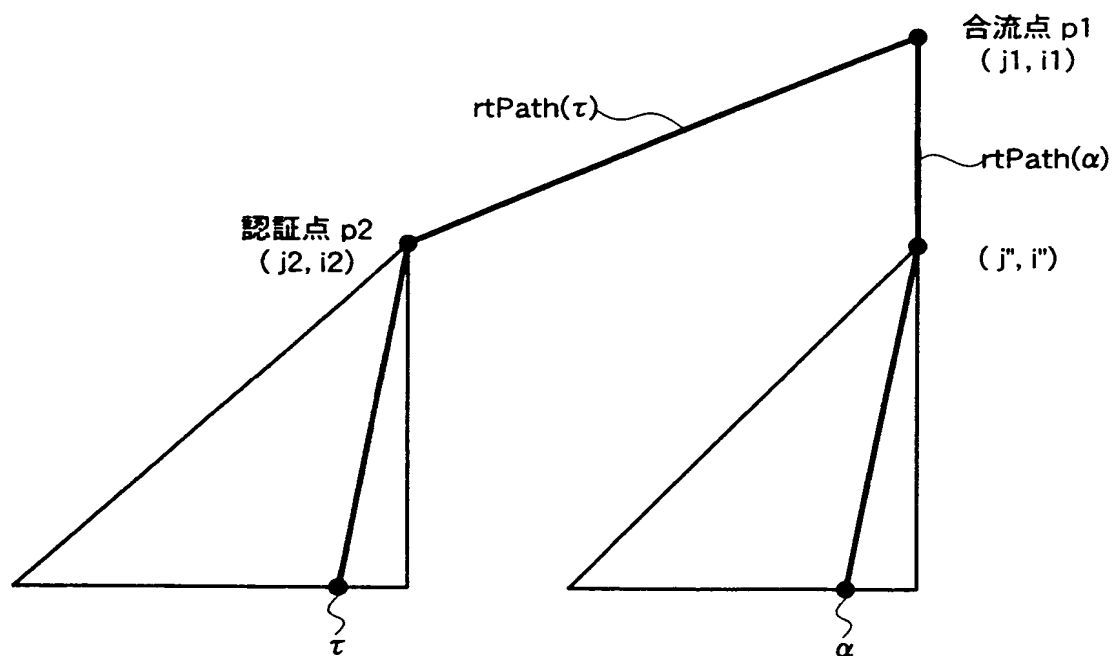
[図9]



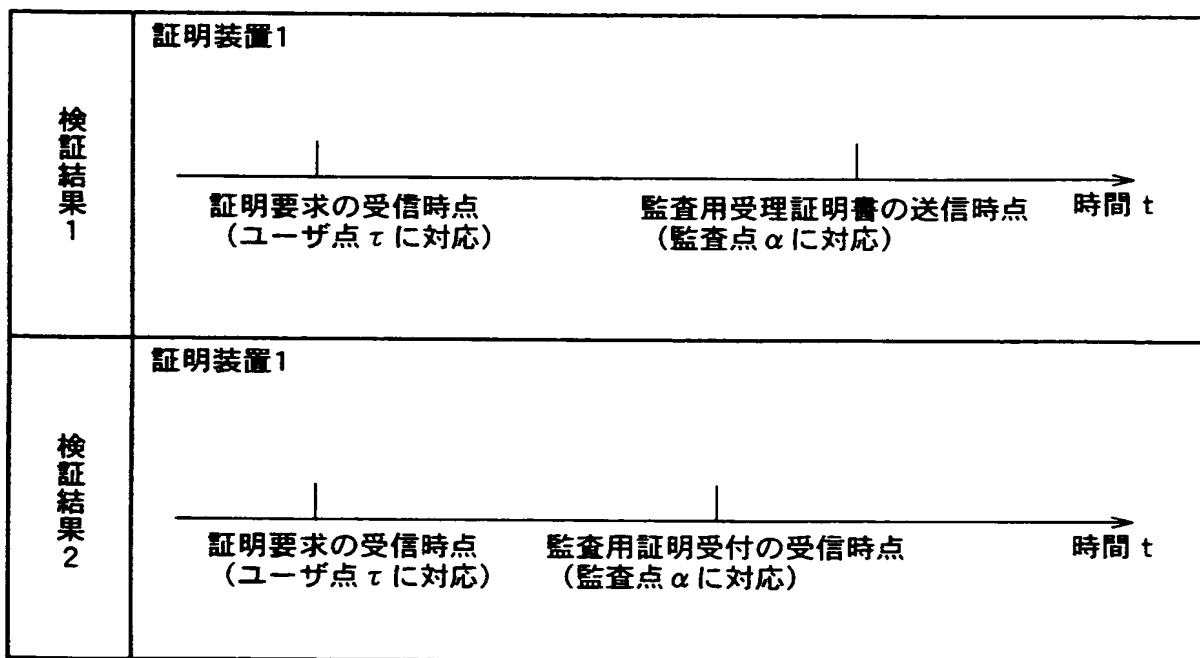
[図10]



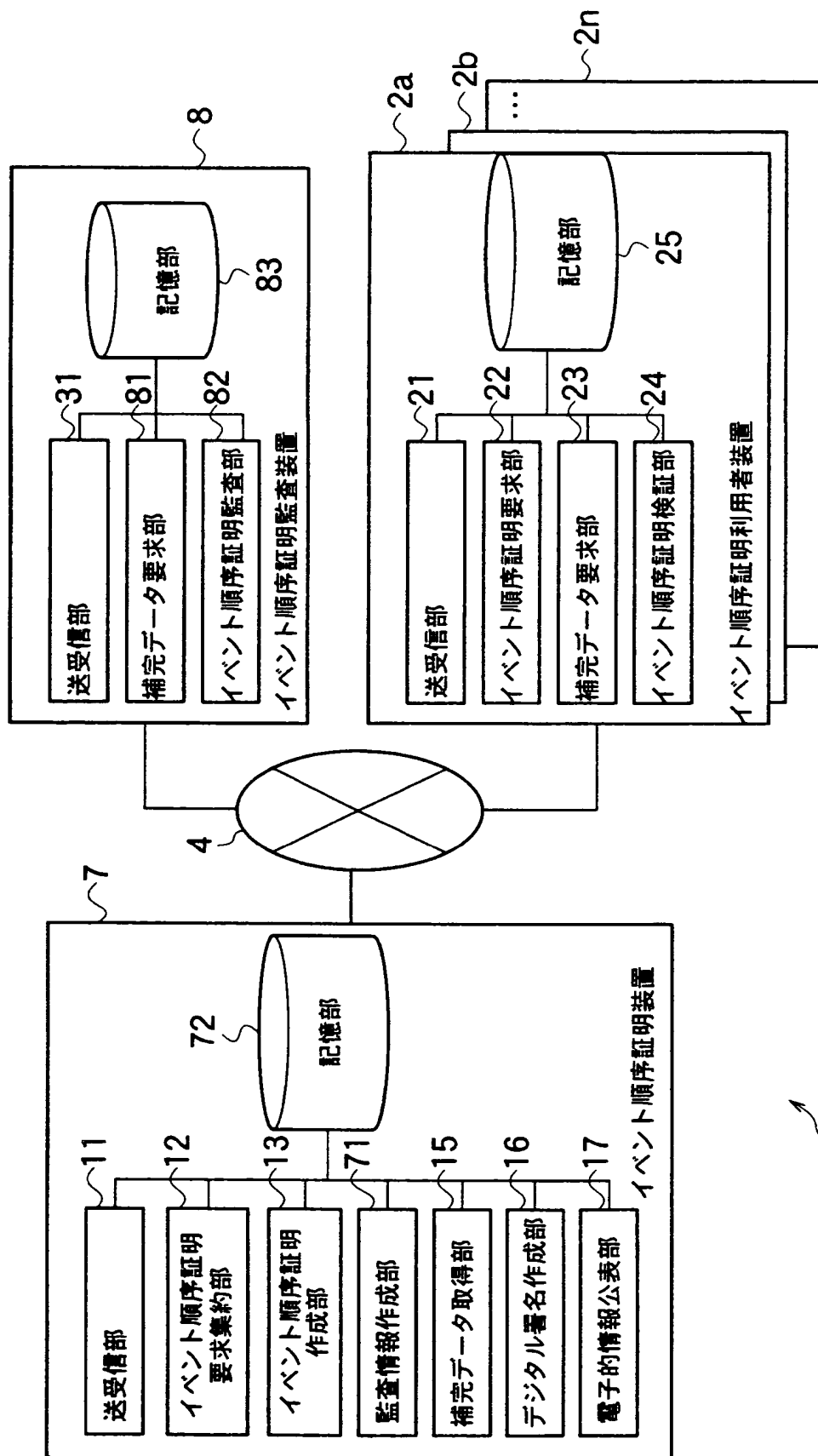
[図11]



[図12]

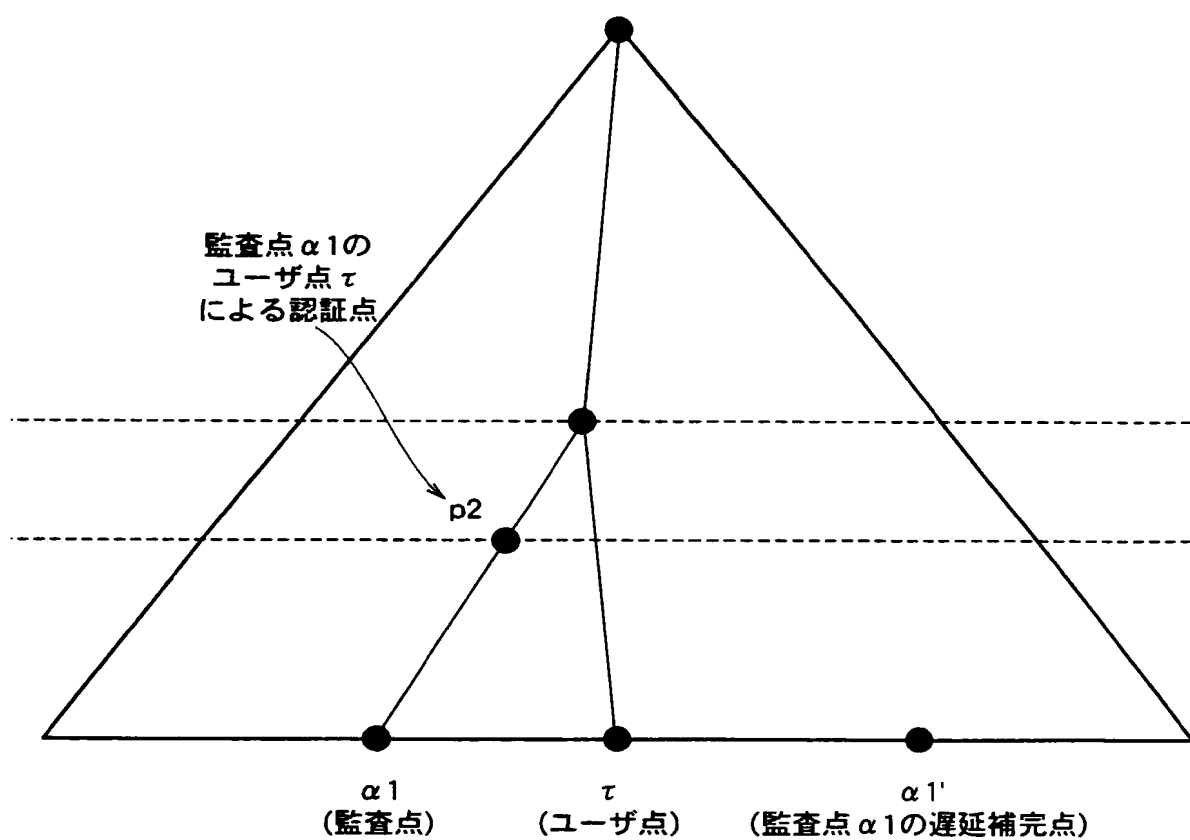


[図13]

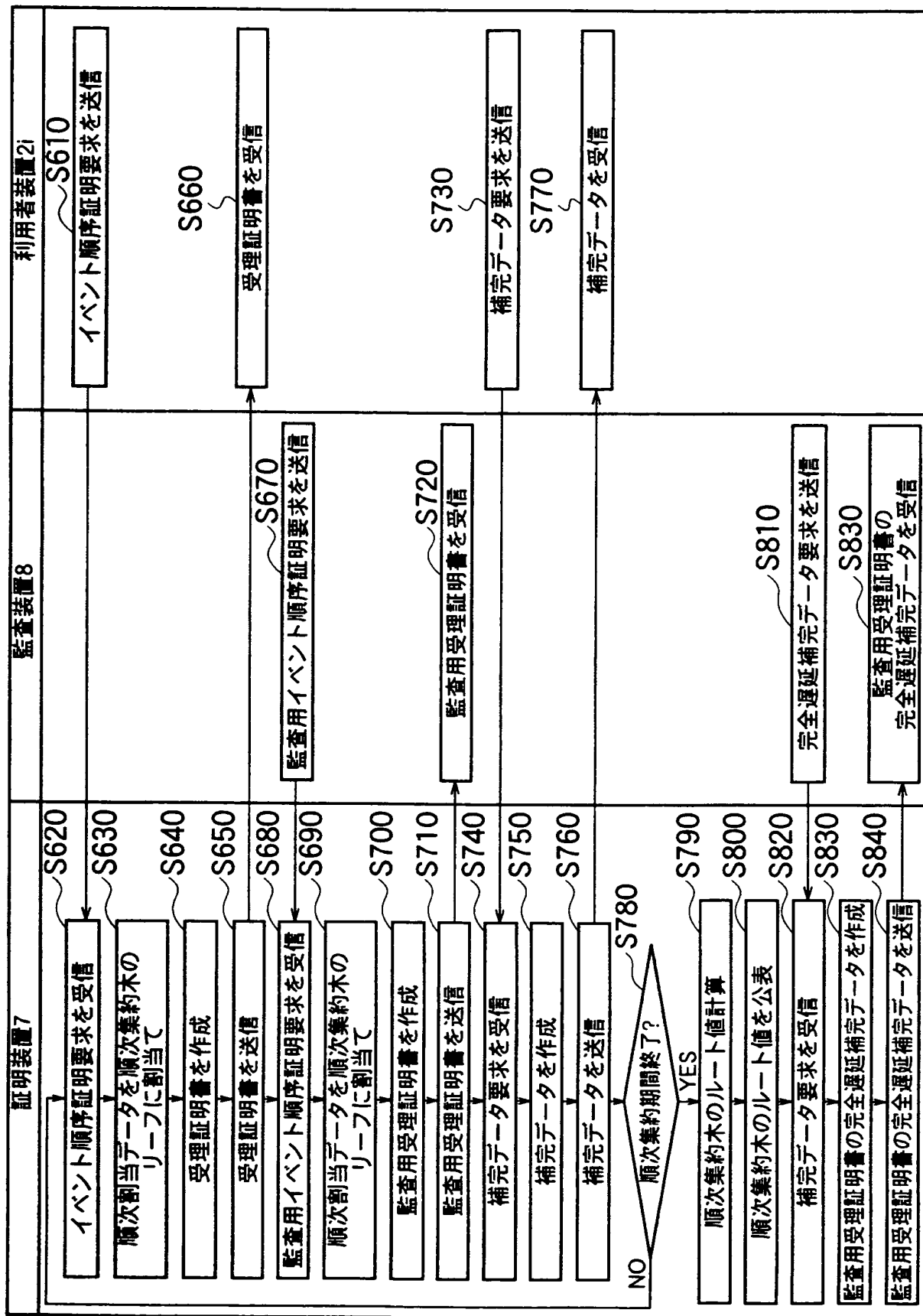


200

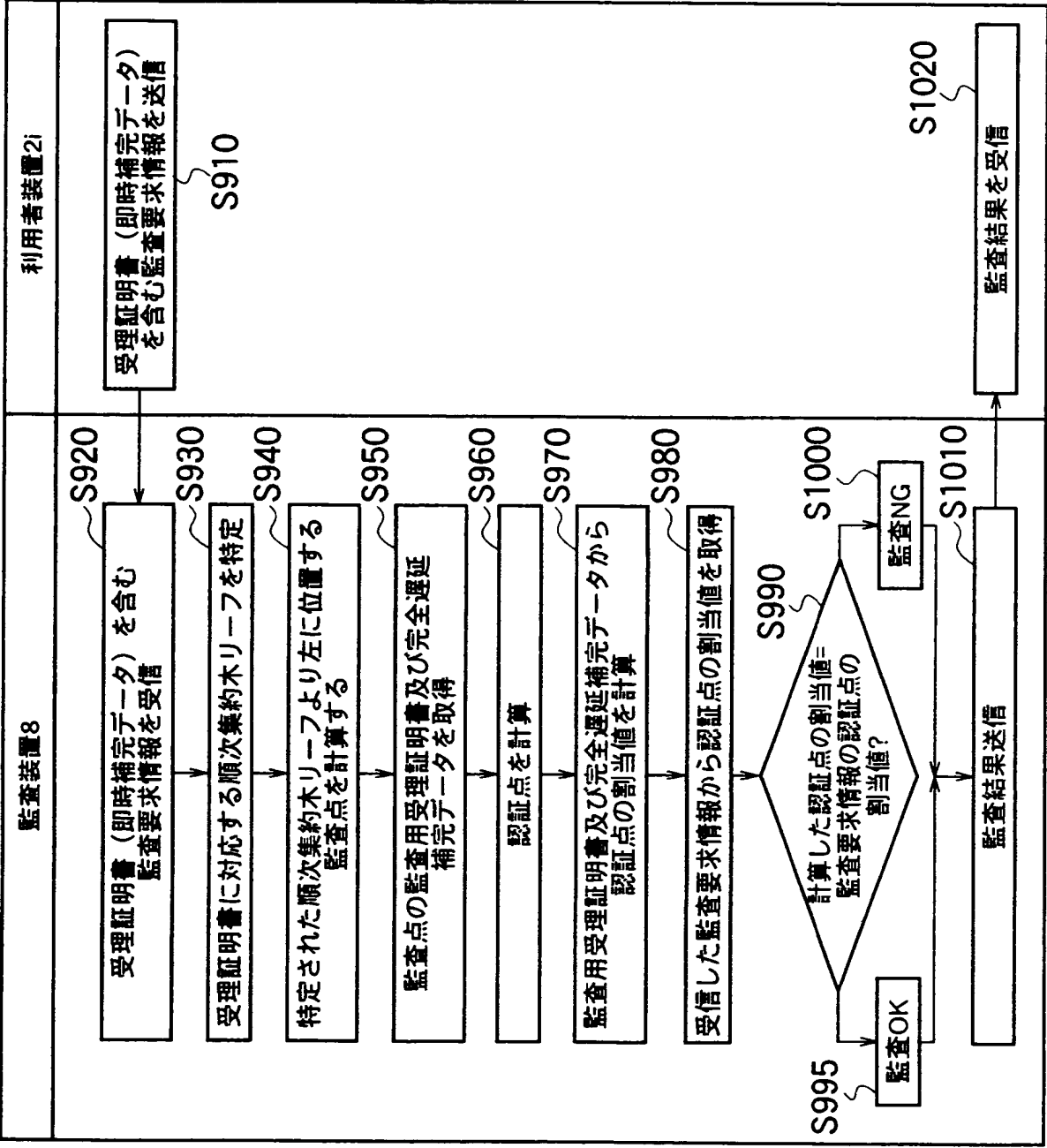
[図14]



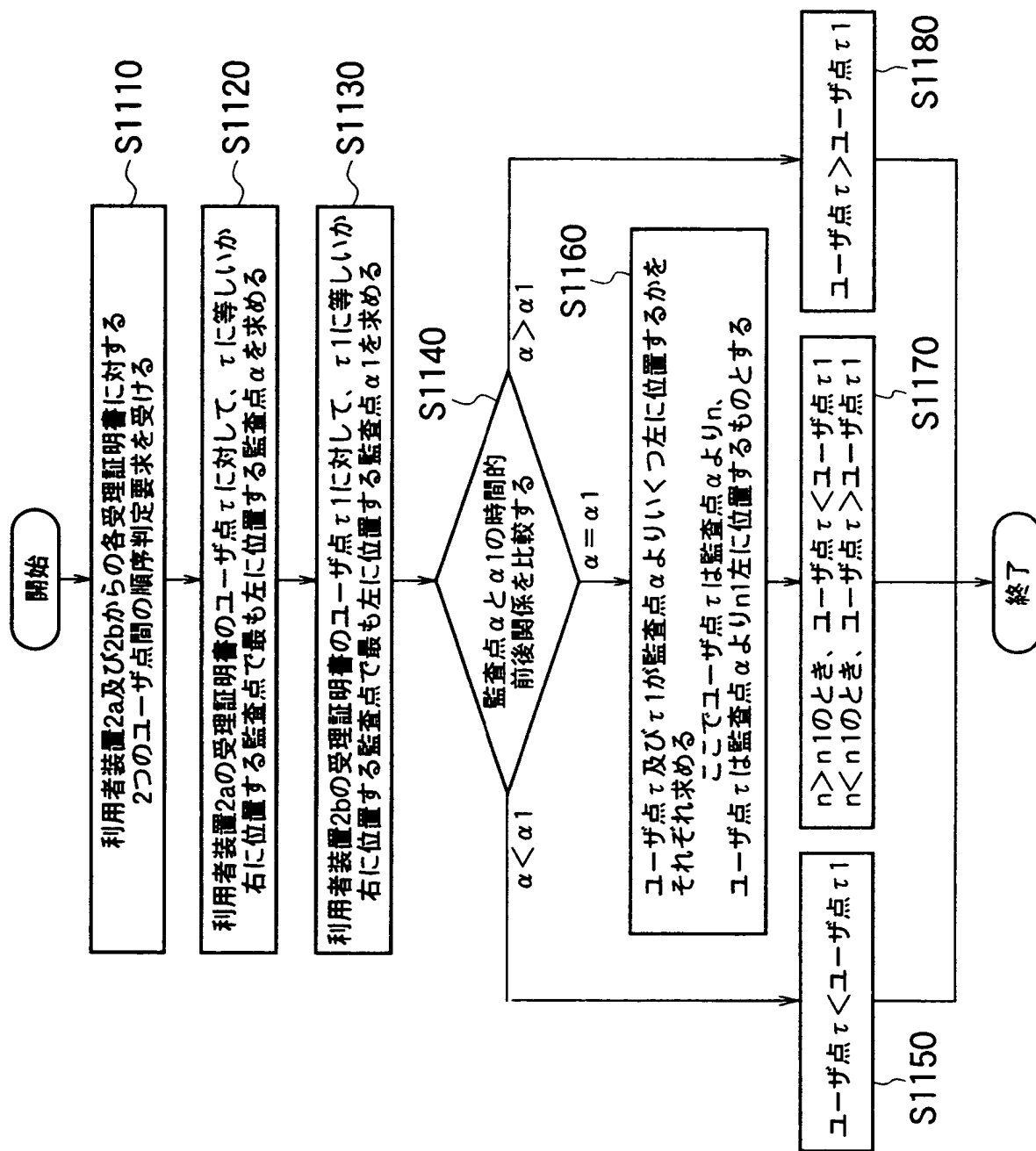
[図15]



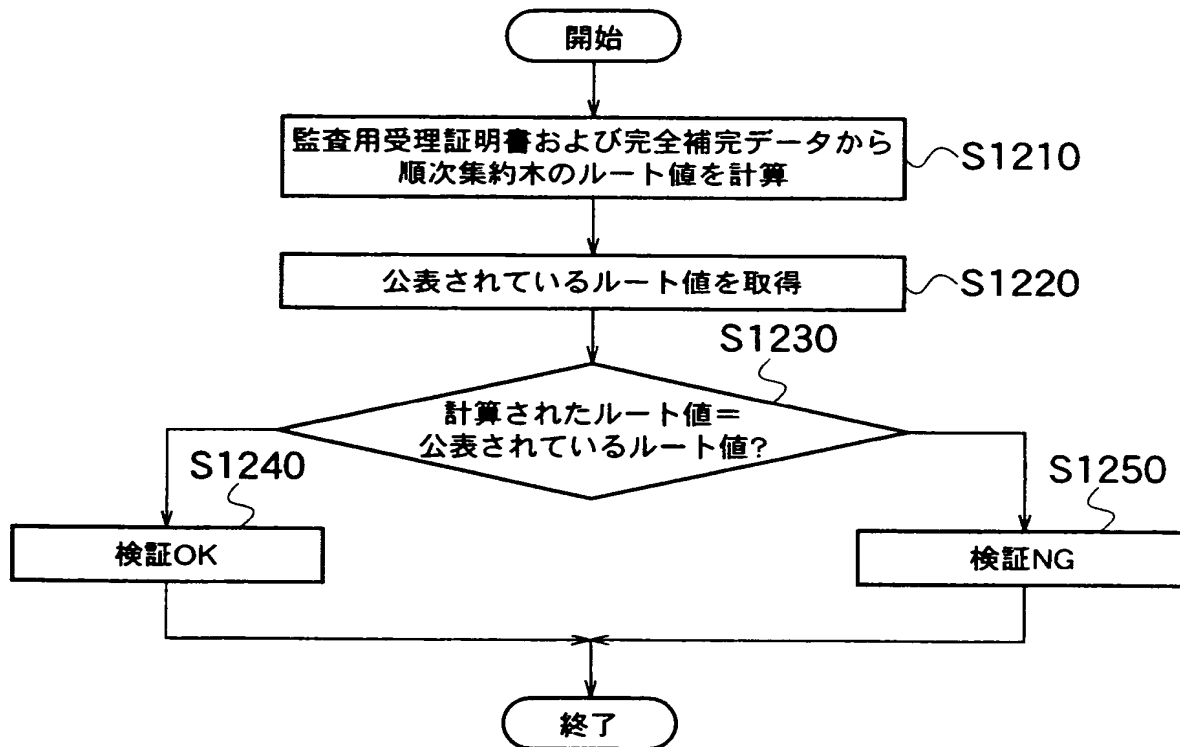
[図16]



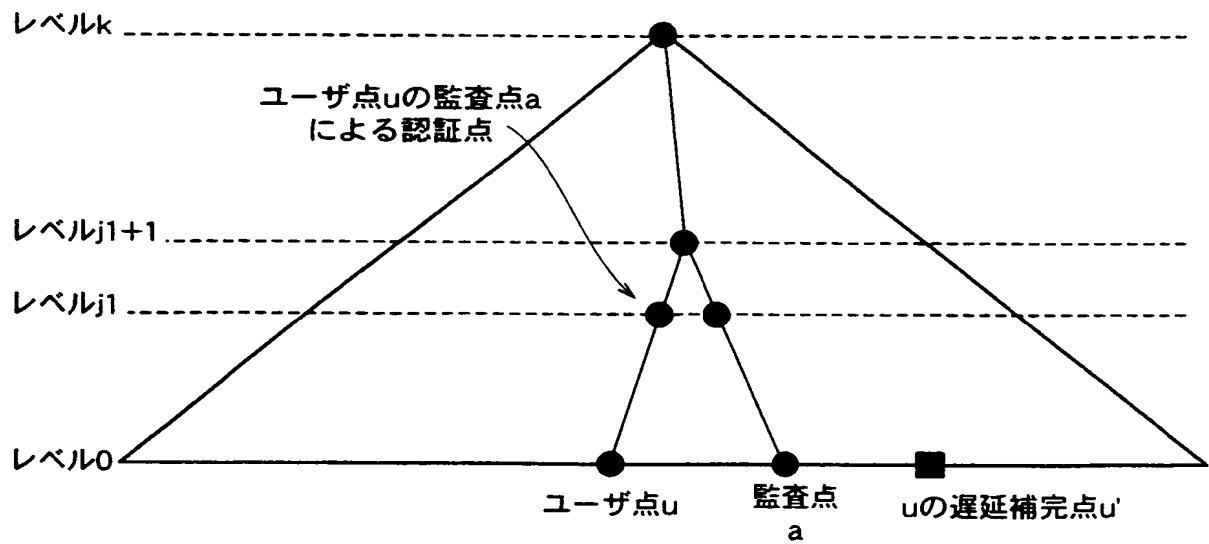
[図17]



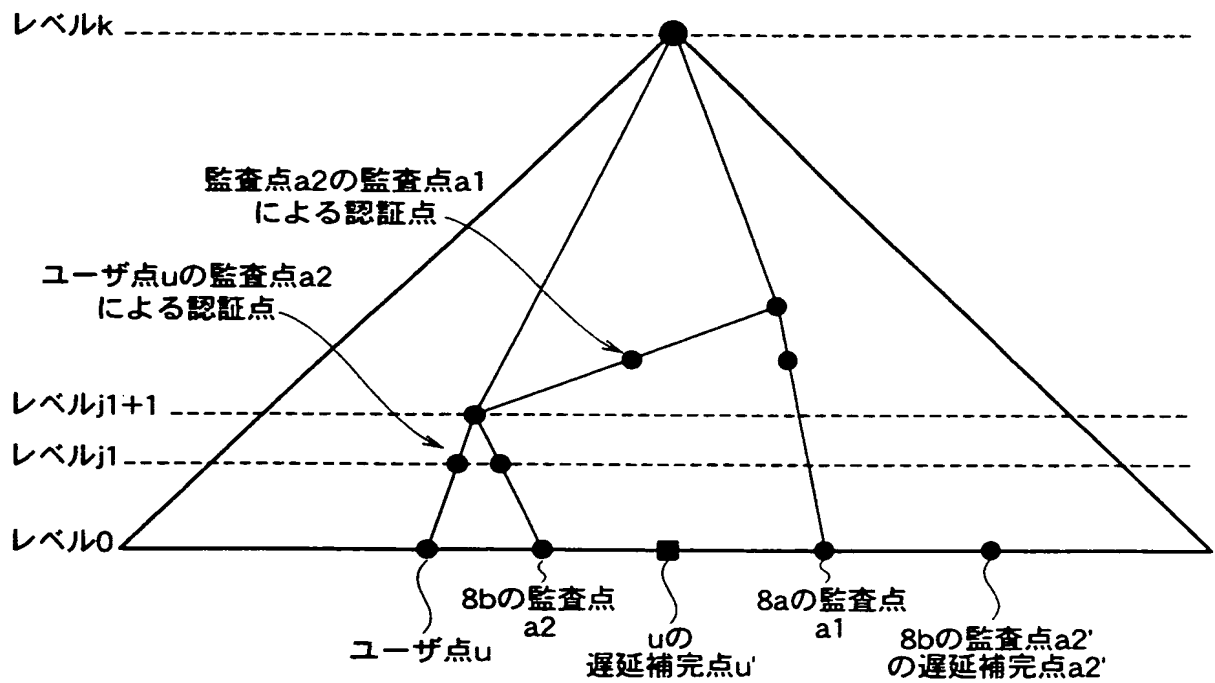
[図18]



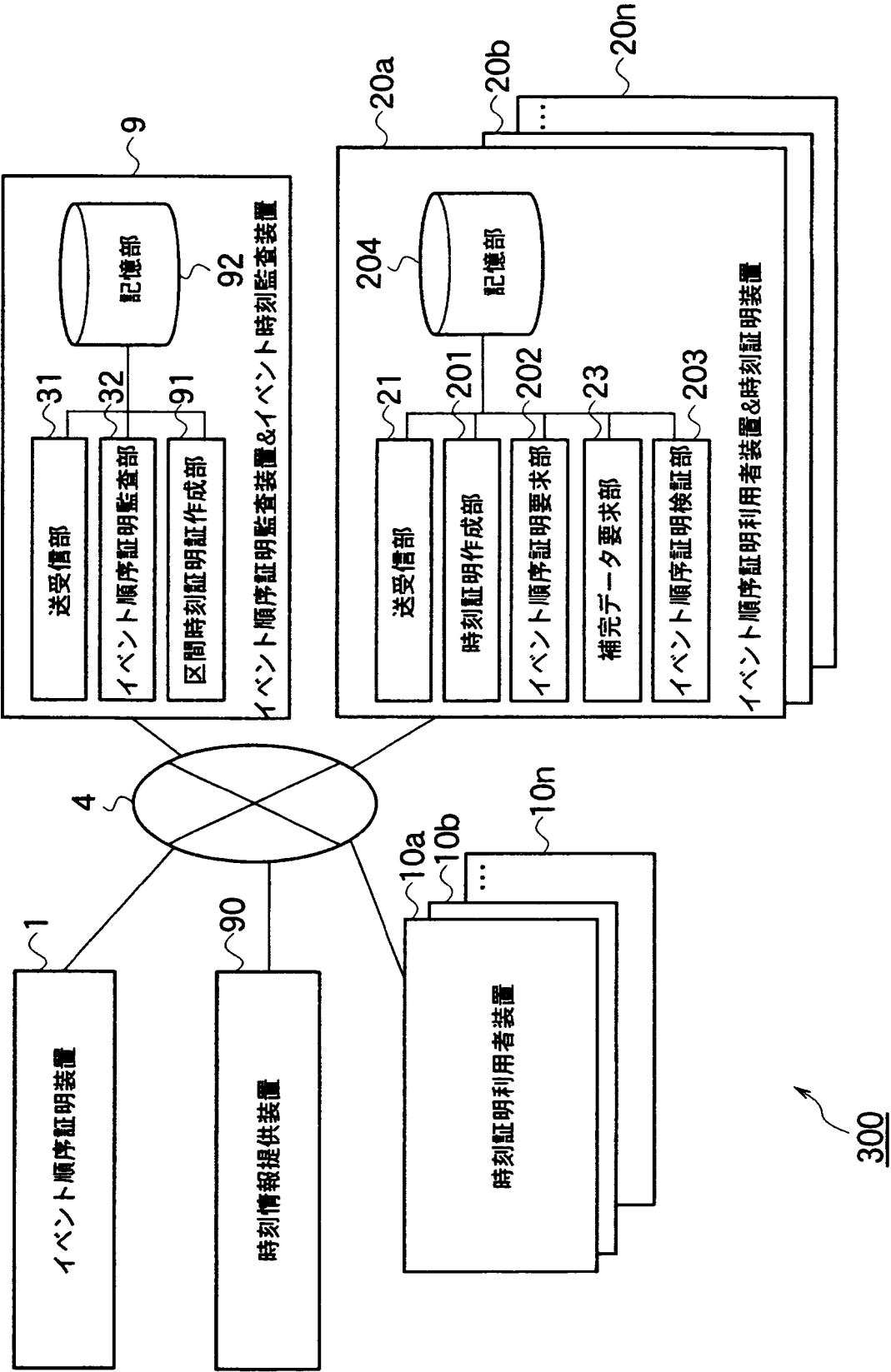
[図19]



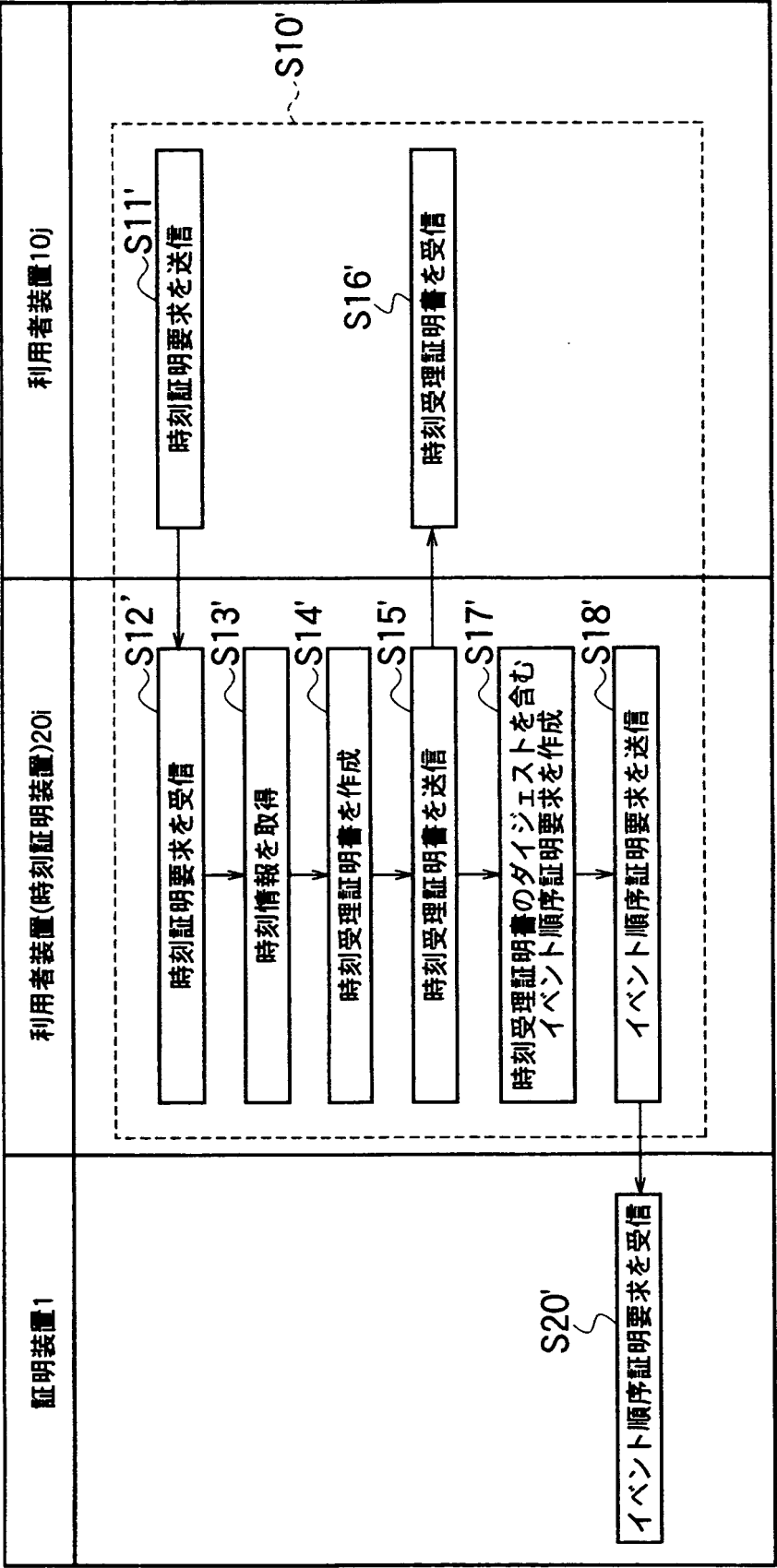
[図20]



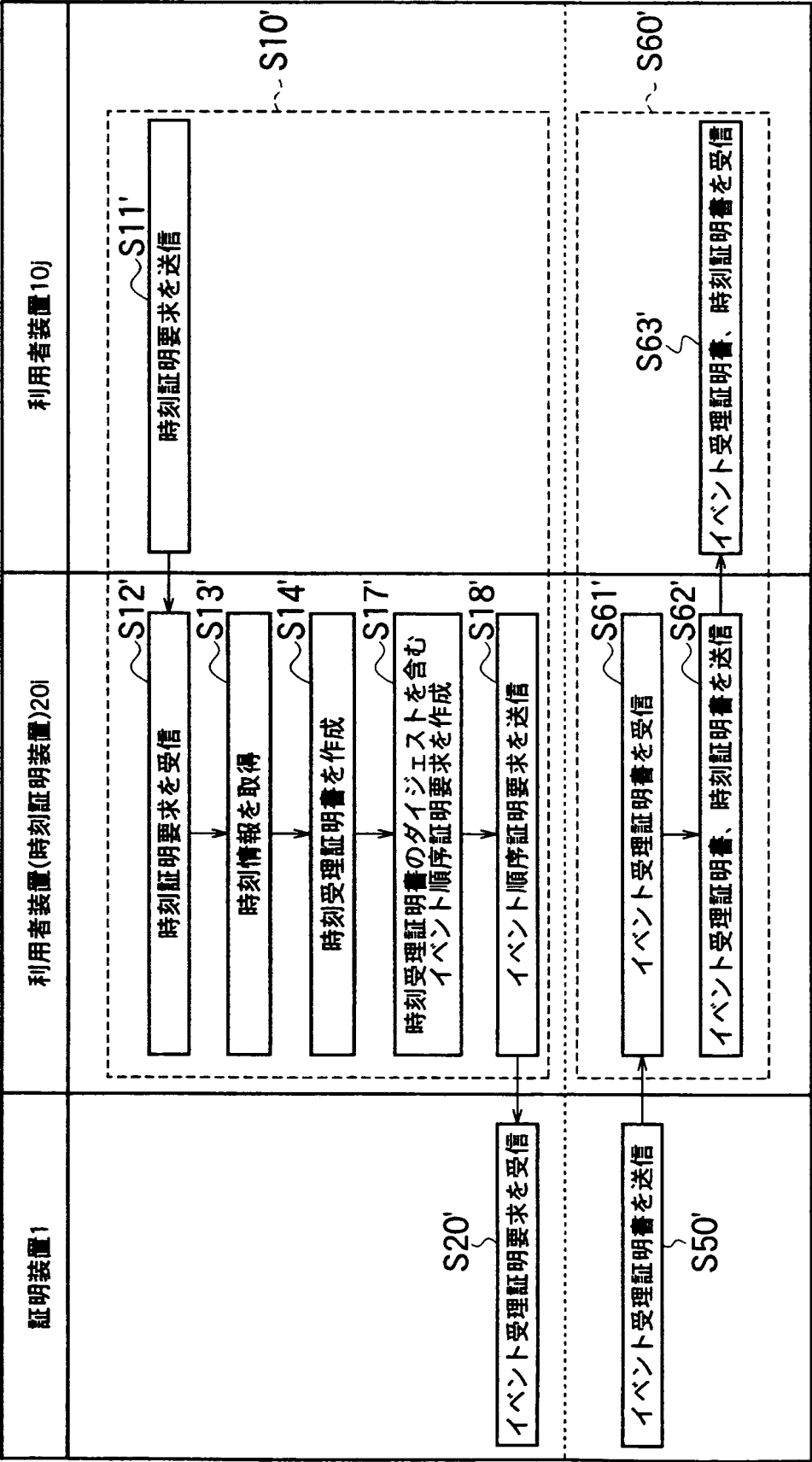
[図21]



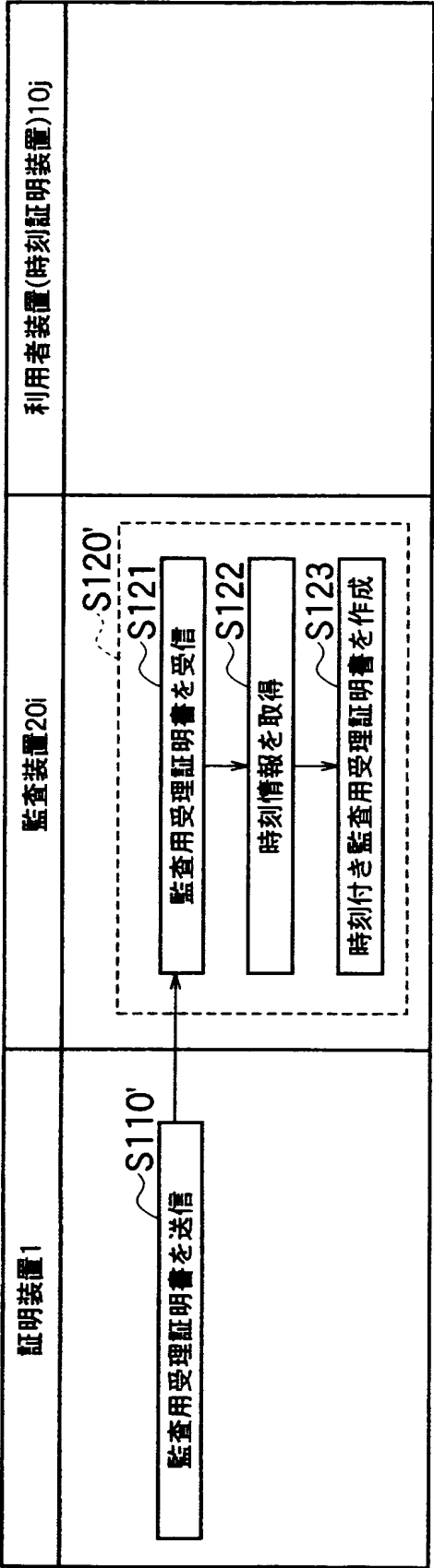
[図22]



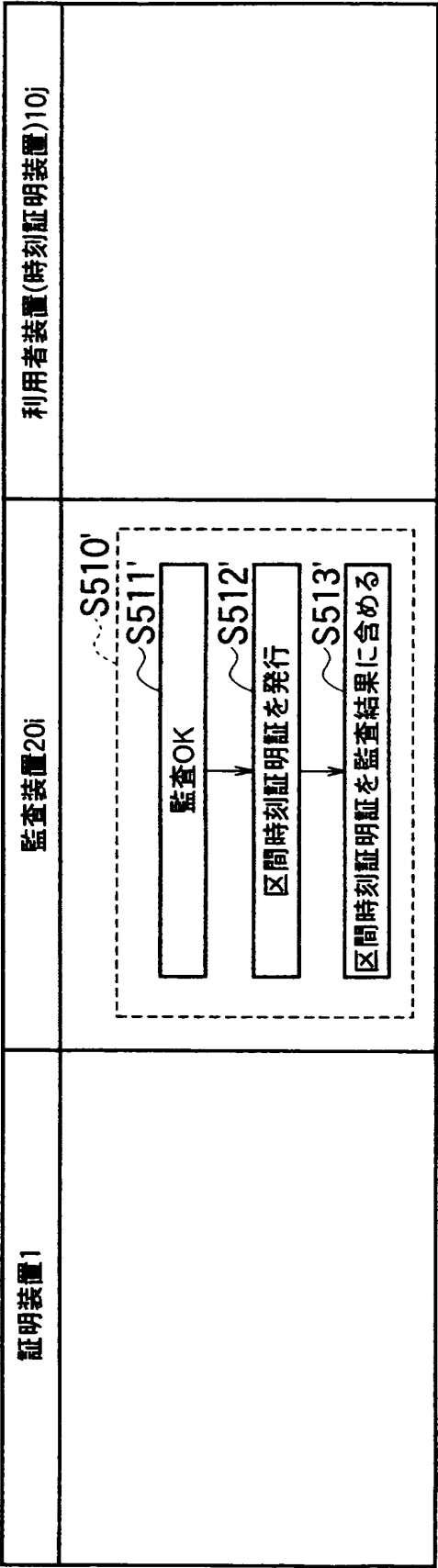
[図23]



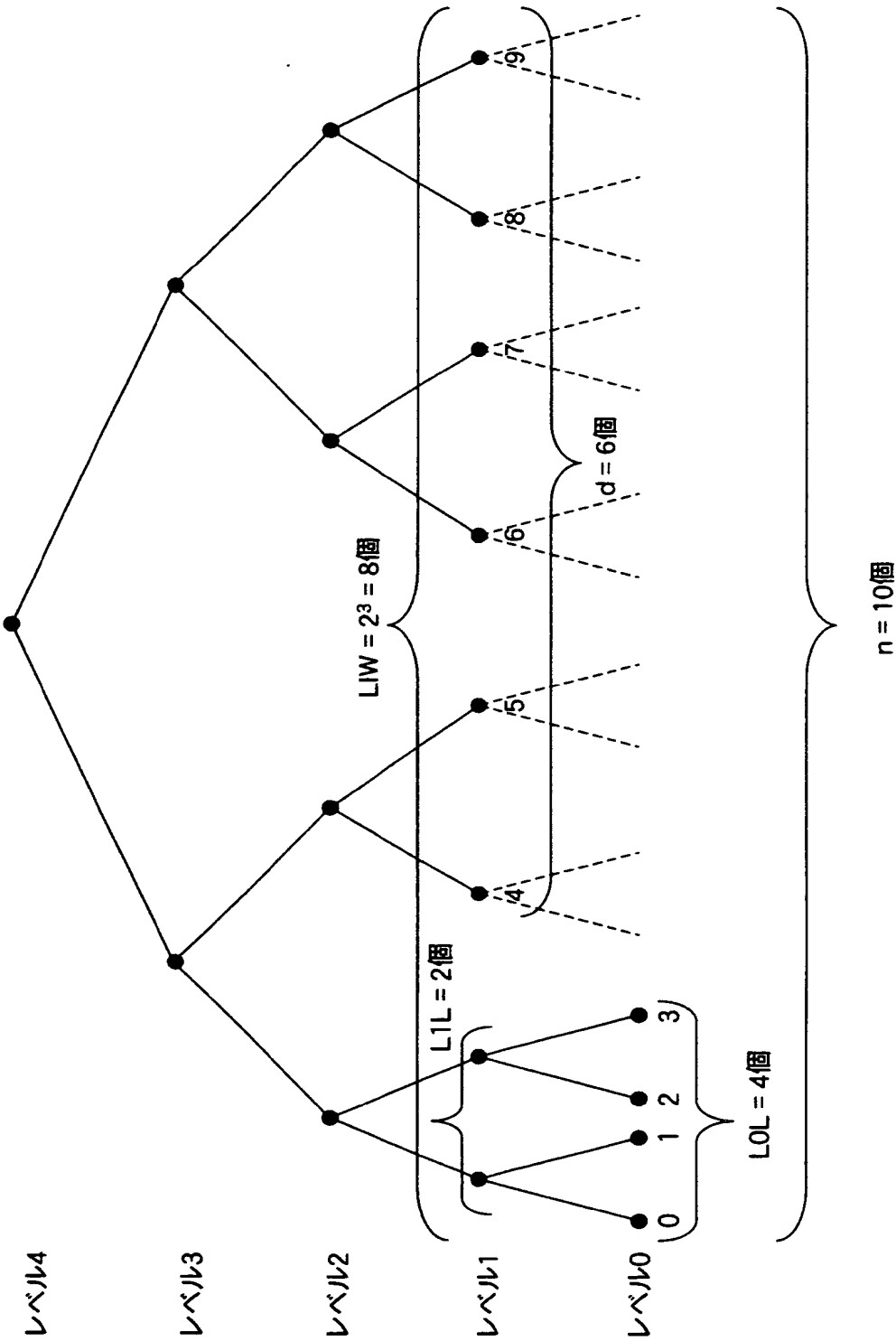
[図24]



[図25]



[図26]



[図27]

(1) ループ1: 構成法その3では、定められた時間間隔が終了するまで以下の処理を繰り返す.

(1.1) 受け付けた要求をxに置く.

(1.2) nを1インクリメントする.

(1.3) ループ2: $j = 0, \dots, K$ に対して以下の処理を行う.

(1.3.1) $i := i_j$ と置く.

(1.3.2) $j = 0$ のときは、 $A_j[i] := x$
(即ち、ノード(j, i_j)にxを設定する).

(1.3.3) $j > 0$ のときは、以下を行う.

- $x0 := A_{j-1}[\text{index}(\text{leftChild}(j, i))]$
(ノード(j, i)のleft-childに割り付けられた値をx0とおく).
- $x1 := A_{j-1}[\text{index}(\text{rightChild}(j, i))]$
(ノード(j, i)のright-childに割り付けられた値をx1とおく).
- $x2 := h(x0 \parallel x1)$ を計算する.
- $A_j[i] := x2$
(即ち、ノード(j, i)にx2を割り付ける).

(1.3.4) i_j を1インクリメントする.

(1.3.5) i_j が偶数のときは、ループ2を抜ける.

ループ2終了.

ループ1終了.

処理手順1

[図28]

(2) 終了時間がきて、ループ1を抜けた後では次の処理を行う。

(2.1) $k := \text{ceiling}(\log_2(n))$ とおく。

(2.2) $\text{rtPath}(k, 0, n-1)$ を計算し、その結果を $((0, r(0)), \dots, (k, r(k)))$ と置く。

(2.3) ループ3: $j = 0, \dots, k$ に対して以下の処理を行う。

(2.3.1) $i = i_j$ とおく。

(2.3.2) $j = 0$ のとき:

(2.3.2.1) i が奇数のとき:

- ・ダミー値 $r := R(0, i)$ を生成する。
- ・ $A_j[i] := r$
(ノード $(0, i)$ に r を割り当て)。
- ・ $b_j := \text{true}$ と置く。
- ・ i_j を1インクリメントする。

(2.3.2) $0 < j \leq k$ のとき:

(2.3.2.1) $i = r(j)$ のとき:

(即ち、ノード (j, i) が $\text{rtPath}(k, 0, n-1)$ 上にあるとき):

(2.3.2.1.1) $x0 := A_{j-1}[\text{index}(\text{leftChild}(j, i))]$

(ノード (j, i) の left-child に割り付けられた値を $x0$ と置く)。

(2.3.2.1.2) $x1 := A_{j-1}[\text{index}(\text{rightChild}(j, i))]$

(ノード (j, i) の right-child に割り付けられた値を $x1$ と置く)。

(2.3.2.1.3) $x2 := h(x0 \parallel x1)$ を計算する

(2.3.2.1.4) $A[j] := x2$

(即ち、ノード (j, i) に $x2$ を割り付ける)。

(2.3.2.1.5) i が偶数で $j < k$ のとき:

- ・ i を1インクリメントする。
- ・ $r := R(j, i)$ を計算し、 $A_j[i] := r$
(即ち、ノード (j, i) に r を割り当てる)。
- ・ $b_j := \text{true}$ と置く。
- ・ $i_j := i+1$ と置く。

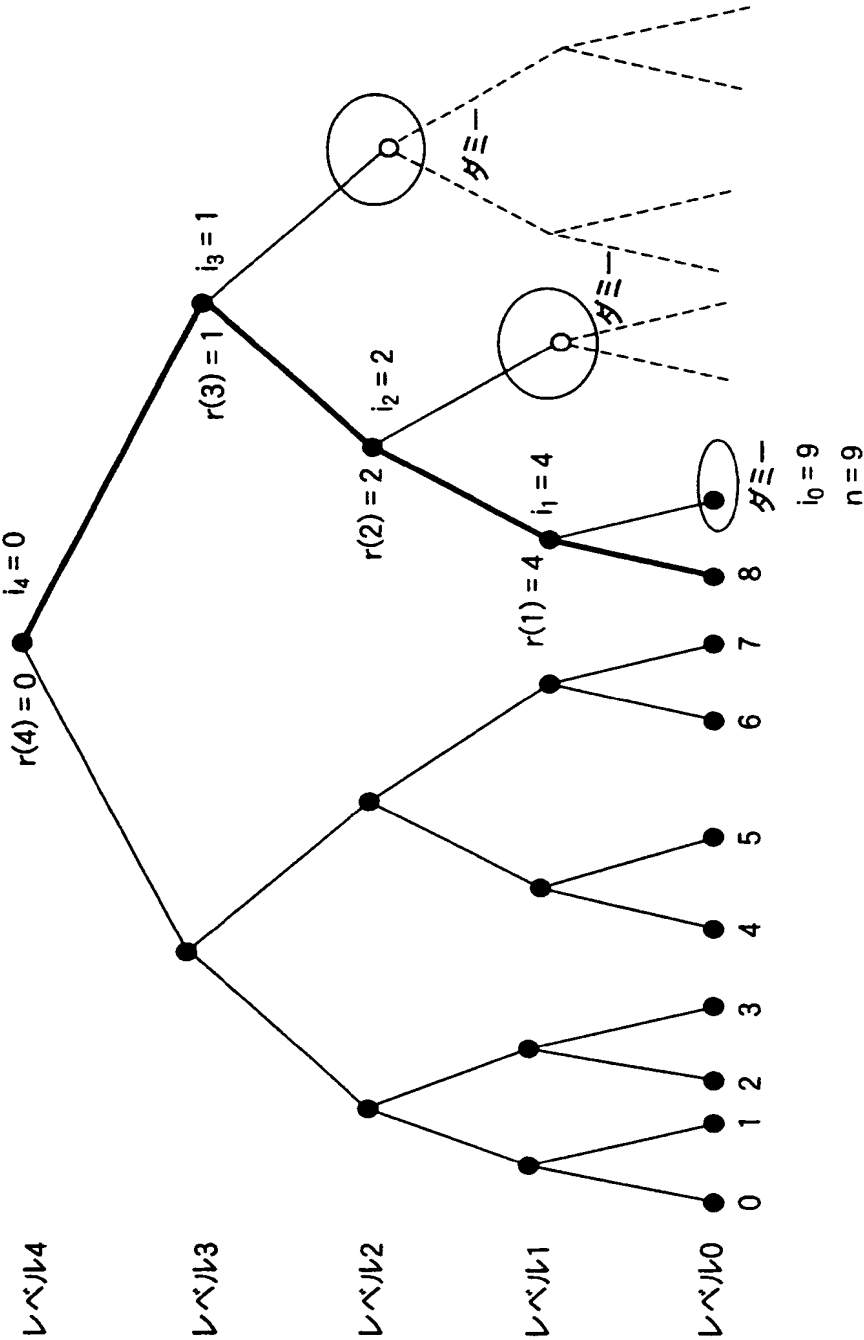
(2.3.2.2) $i = r(j)+1$ で i が奇数で $j < k$ のとき:

- ・ $r := R(j, i)$ を計算し、 $A_j[i] := r$
(即ち、ノード (j, i) に r を割り当てる)。
- ・ $b_j := \text{true}$ と置く。
- ・ i_j を1インクリメントする。

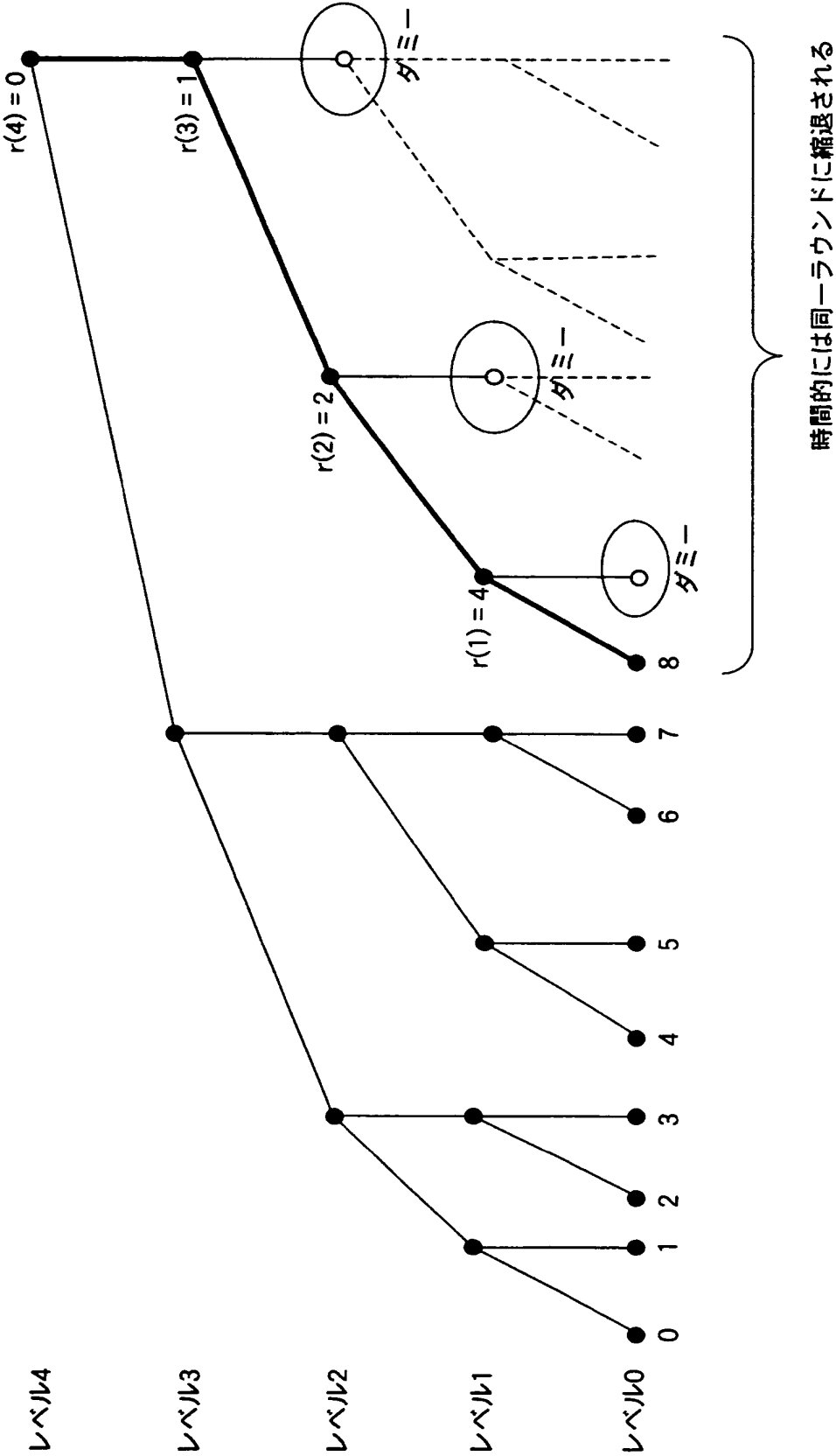
ループ3終了。

処理
手順
2

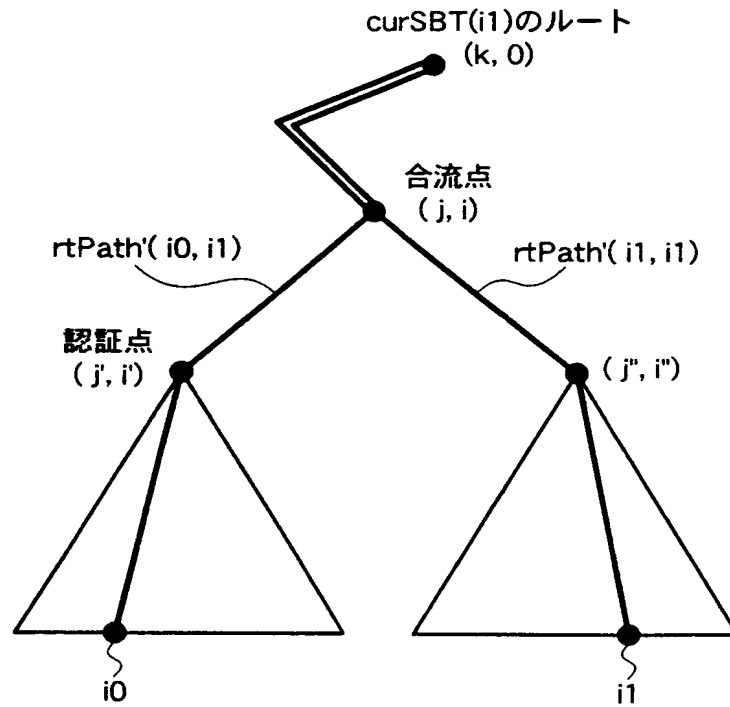
[図29]



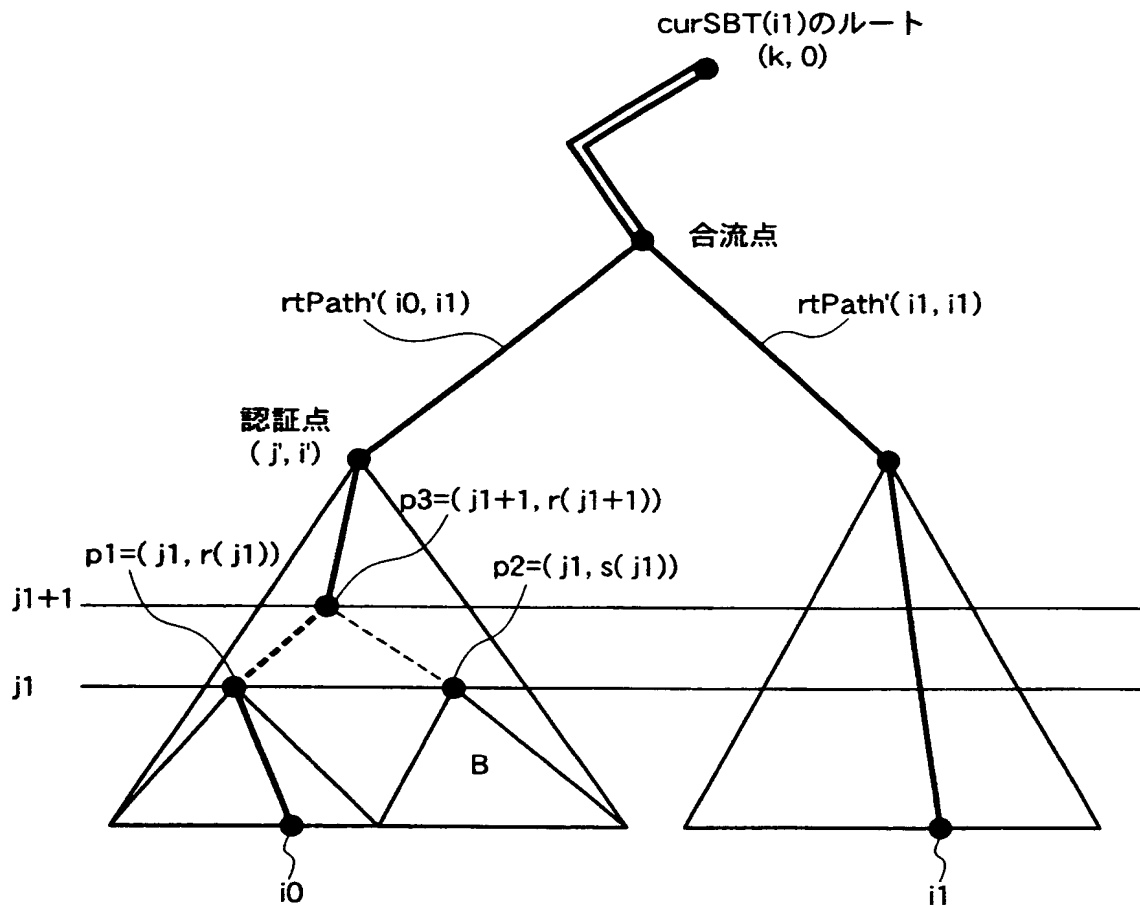
[図30]



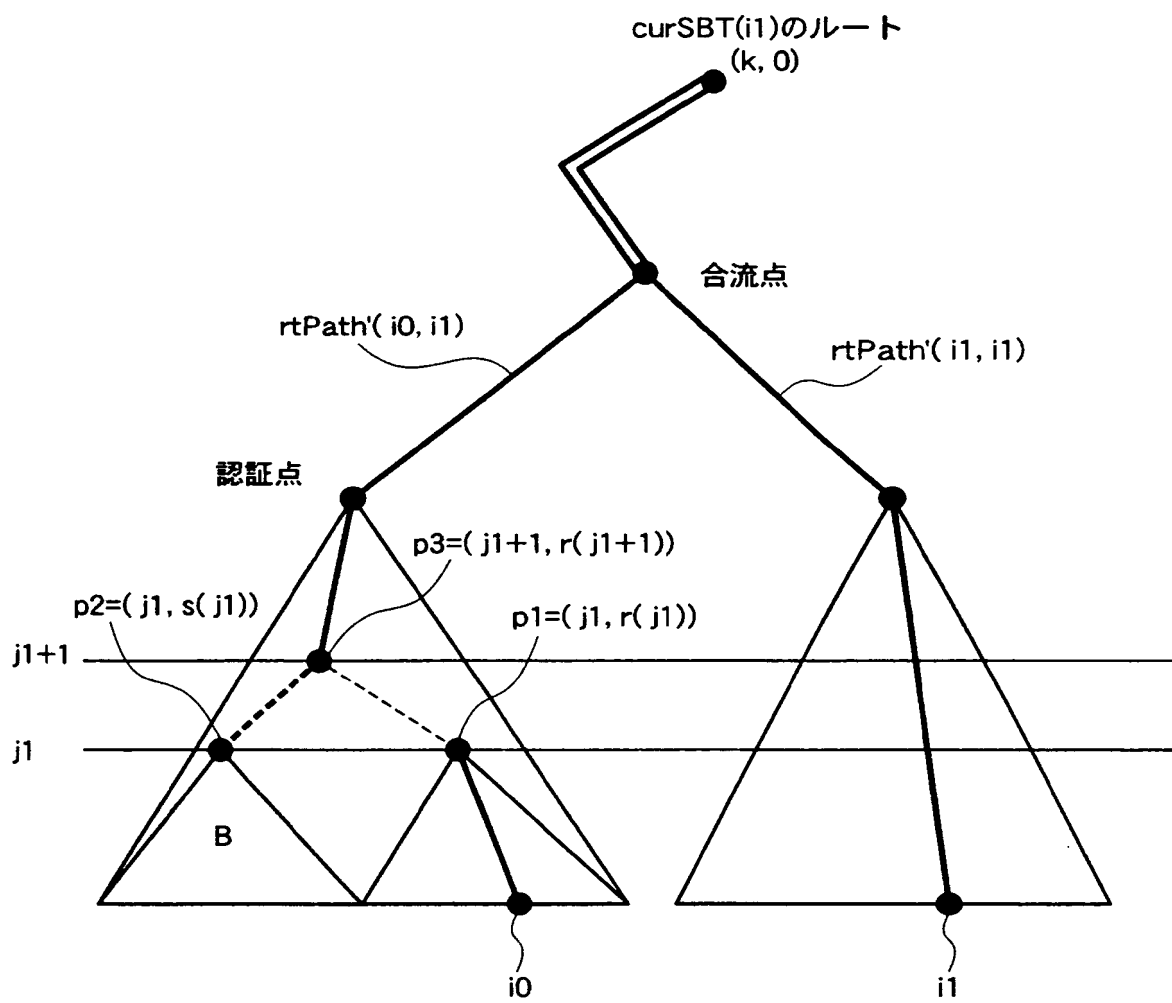
[図31]



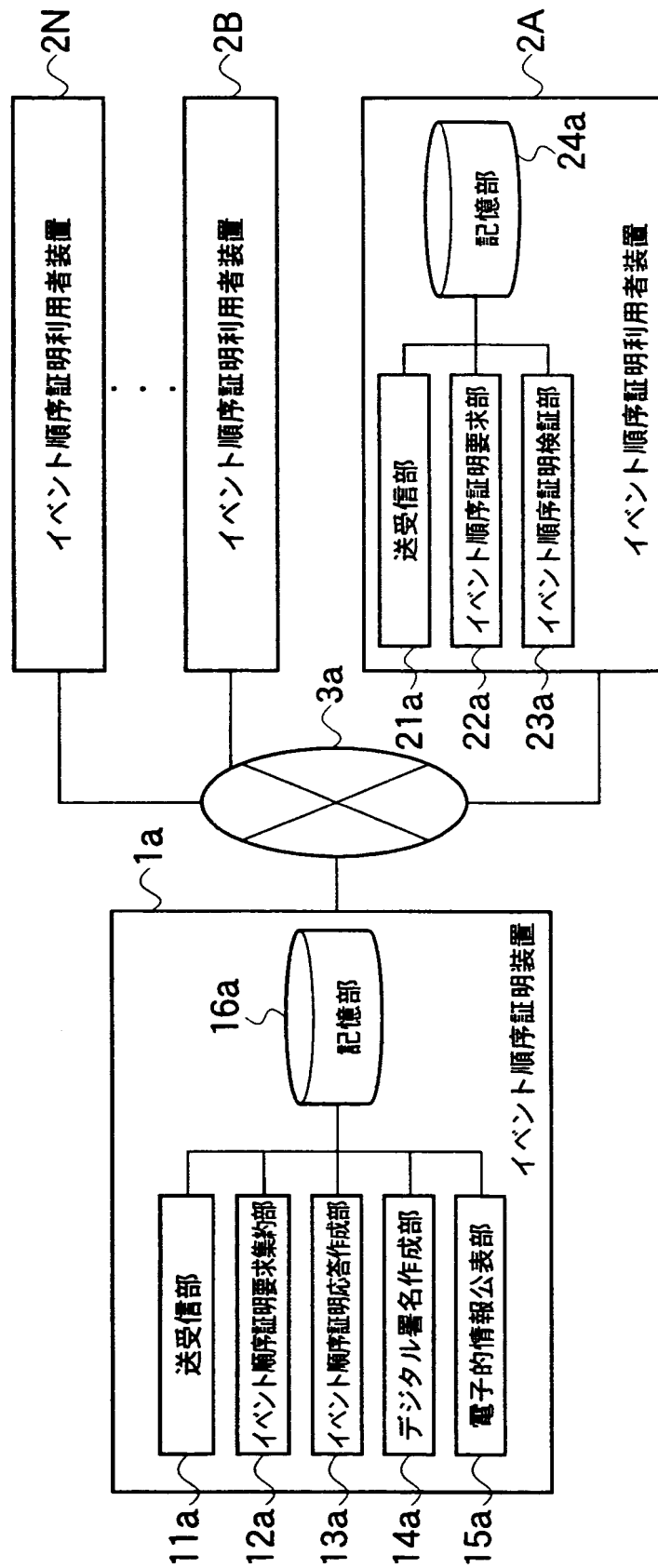
[図32]



[図33]

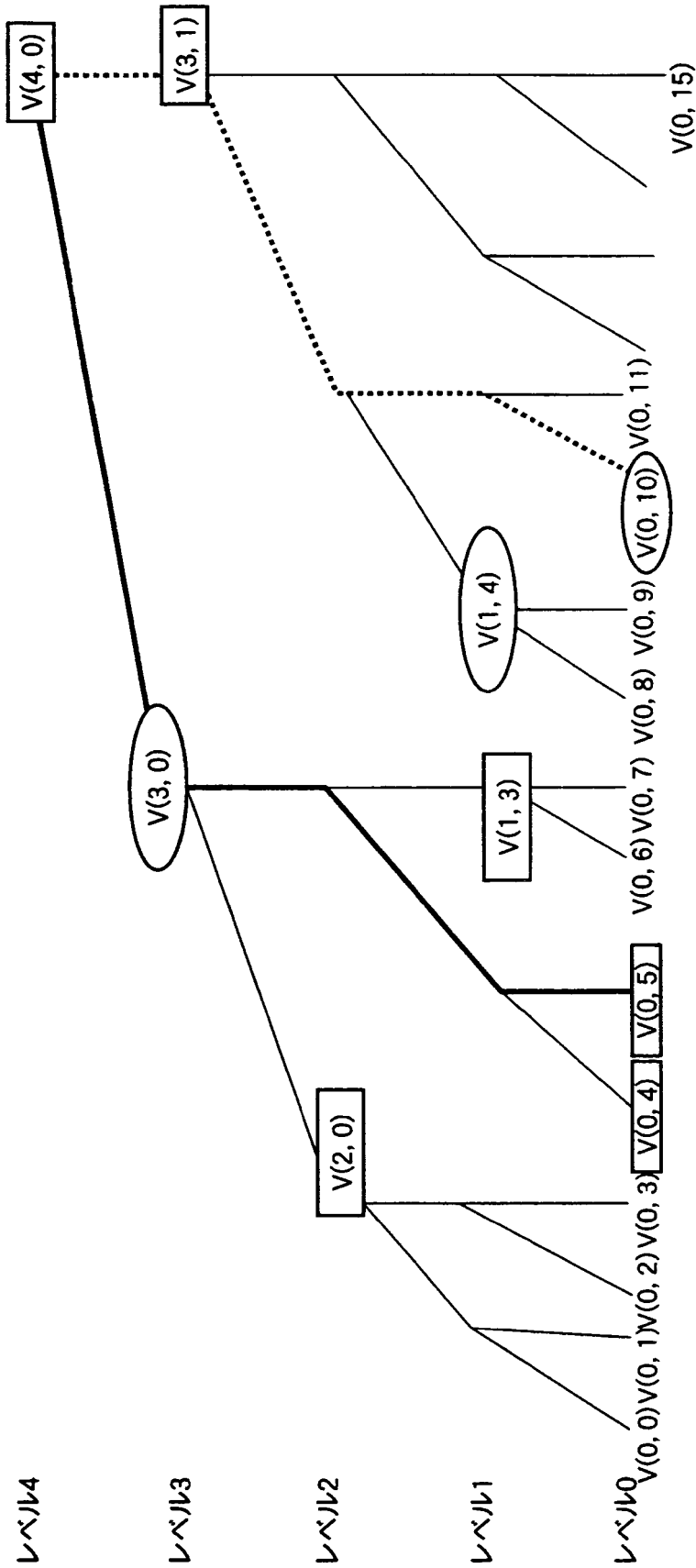


[図34]



100a

[図35]

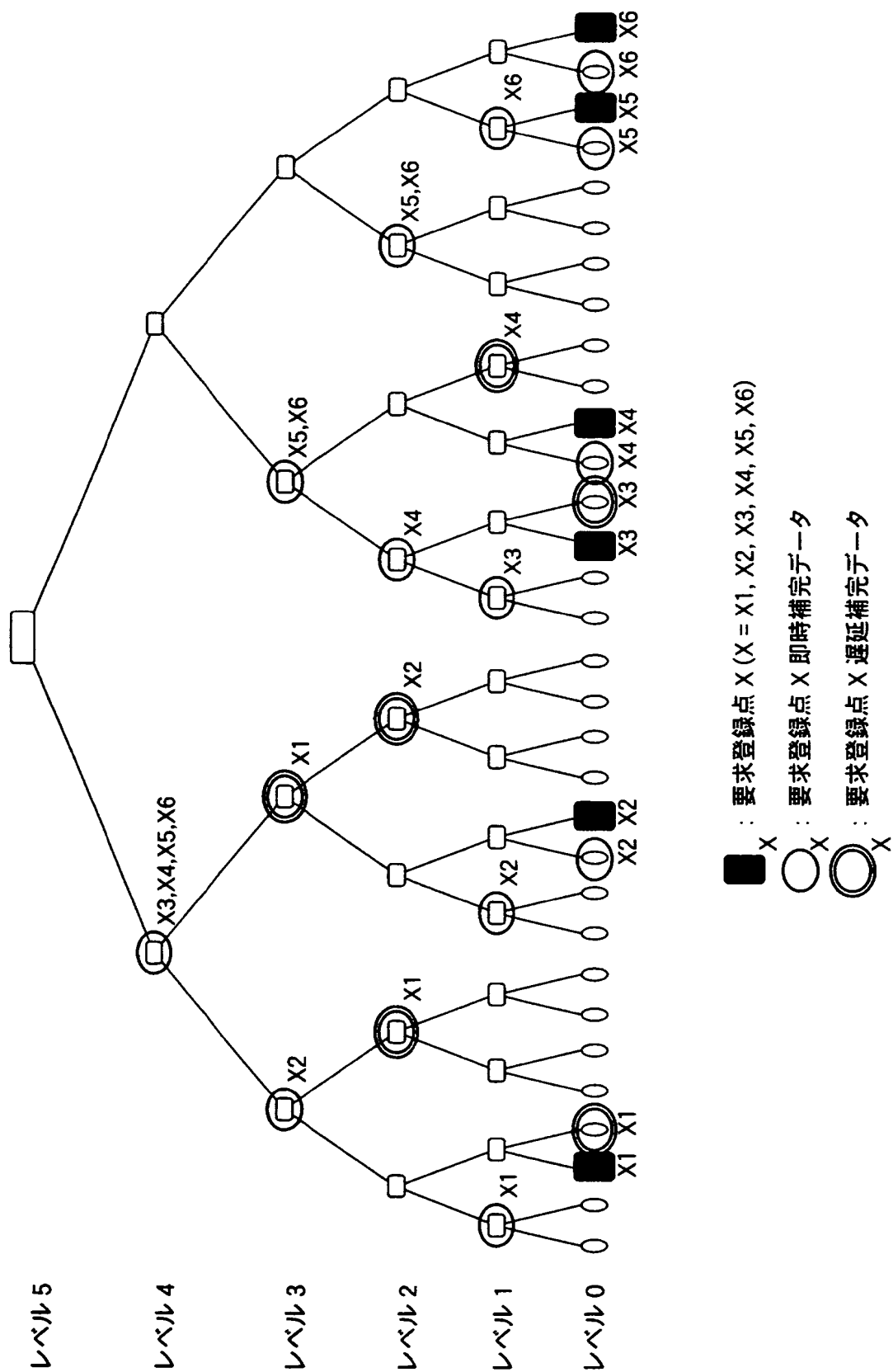


[図36]

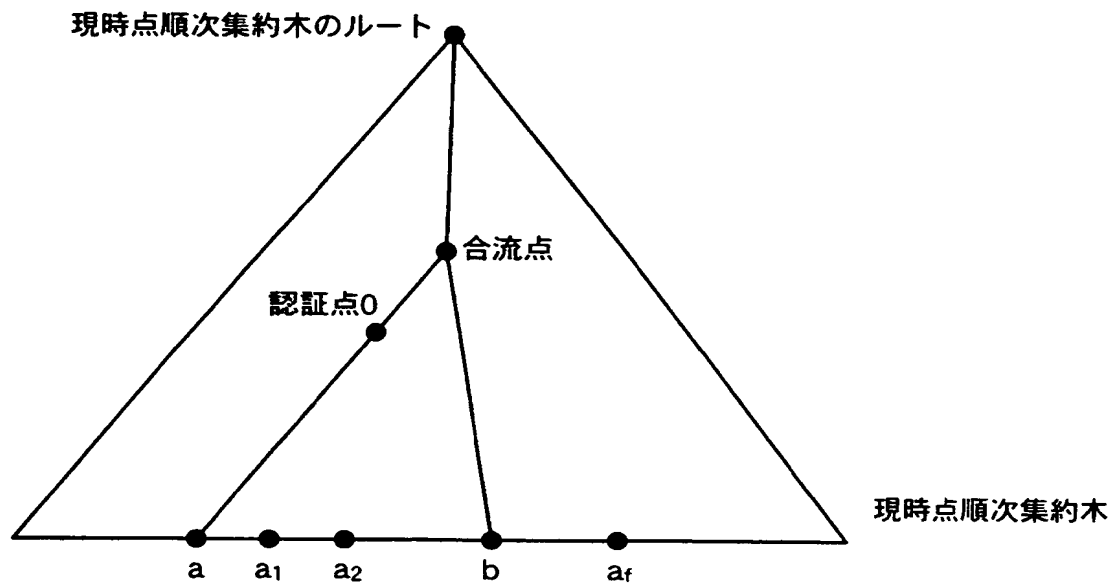
項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木番号	n	○
順次集約木リーフ番号	i	○
登録点の即時補完データ(位置情報、割当値)	SK	○
過去の各登録点の遅延補完データ(位置情報、割当値)	TK	○

イベント順序受理証明書
EOC(y)

[図37]



[図38]



[図39]

